



# **ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ (ИБРР-2025)**

**XIV САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ**

*Санкт-Петербург, 29-31 октября-2025 г.*

## **МАТЕРИАЛЫ КОНФЕРЕНЦИИ**

**Санкт-Петербург  
2025**



# **ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ (ИБРР-2025)**

**XIV САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ**

*Санкт-Петербург, 29-31 октября-2025 г.*

## **МАТЕРИАЛЫ КОНФЕРЕНЦИИ**

**Санкт-Петербург**

**2025**

УДК (002:681):338.98

И 74

И 74

**Информационная безопасность регионов России (ИБРР-2025).**

XIV Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 29-31 октября-2025 г.: Материалы конференции / СПОИСУ. – СПб., 2025. – 551 с.

**ISBN 978-5-00182-159-5**

Сборник охватывает широкий круг направлений: Государственная политика обеспечения информационной безопасности регионов России; Правовые аспекты информационной безопасности; Безопасность информационных технологий; Информационная безопасность телекоммуникационных сетей; Информационно-экономическая безопасность, Информационная безопасность транспортных систем; Информационная безопасность объектов морской техники и морской инфраструктуры; Информационно-психологическая безопасность; Информационная безопасность в социокomпьютинге; Информационная безопасность киберфизических систем; Информационная безопасность геоинформационных систем; Подготовка и переподготовка кадров в области обеспечения информационной безопасности, а также молодежных научных школ «Экосистема безопасных городских цифровых сервисов», «Безопасные интеллектуальные информационные системы и технологии», «Безопасные системы связи». Предназначен для широкого круга руководителей и специалистов органов государственной власти, академических учреждений, высших учебных заведений, научно-исследовательских и научно-производственных предприятий и организаций Санкт-Петербурга и других регионов, специализирующихся в области информатизации, связи и защиты информации.

УДК (002:681):338.98

Редакционная коллегия: *Б.Я. Советов, В.В. Касаткин*

Компьютерная верстка и дизайн: *А.С. Михайлова*

Публикуется в авторской редакции

Подписано в печать 15.10.2025. Формат 60x84<sup>1</sup>/<sub>8</sub>. Бумага офсетная.

Печать – ризография. Усл. печ. л. 64. Тираж 500 экз. Заказ № 1372

Отпечатано в ООО «ИПЦ «Измайловский»

190005, Санкт-Петербург, Измайловский пр., 18-д

ISBN 978-5-00182-159-5



**ISBN 978-5-00182-159-5**

© Санкт-Петербургское Общество информатики,  
вычислительной техники, систем связи  
и управления (СПОИСУ), 2025 г.

© Авторы, 2025 г.



# **INFORMATION SECURITY OF RUSSIAN REGIONS (ISRR-2025)**

**XIV ST. PETERSBURG INTERREGIONAL CONFERENCE**

*St. Petersburg, October 29-31, 2025*

## **PROCEEDINGS OF THE CONFERENCE**

**St. Petersburg**

**2025**





## УЧРЕДИТЕЛИ КОНФЕРЕНЦИИ

- Правительство Санкт-Петербурга
- Законодательное Собрание Санкт-Петербурга
- Правительство Ленинградской области
- Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
- Министерство науки и высшего образования Российской Федерации
- Российская академия образования
- Отделение нанотехнологий и информационных технологий Российской академии наук
- Санкт-Петербургское отделение Российской академии наук
- Ассоциация промышленных предприятий Санкт-Петербурга
- Санкт-Петербургская территориальная группа Российского национального комитета по автоматическому управлению
- Санкт-Петербургский Федеральный исследовательский центр Российской академии наук
- Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления

## СОУСТРОИТЕЛИ КОНФЕРЕНЦИИ

- Военная академия связи им. С.М. Буденного
- Военная ордена Жукова академия войск национальной гвардии Российской Федерации
- ВУНЦ ВМФ «Военно-морская академия имени Адмирала Флота Советского Союза Н. Г. Кузнецова»
- Государственный университет морского и речного флота имени адмирала С.О. Макарова
- Дом ученых им. М. Горького
- Российский государственный гидрометеорологический университет
- Санкт-Петербургский государственный морской технический университет
- Санкт-Петербургский государственный университет аэрокосмического приборостроения
- Санкт-Петербургский государственный университет телекоммуникаций им. профессор М.А. Бонч-Бруевича
- Санкт-Петербургский государственный экономический университет
- Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
- Санкт-Петербургский институт экономики и бизнеса
- Санкт-Петербургский информационно-аналитический центр
- Санкт-Петербургский научный центр Российской академии наук
- Санкт-Петербургский политехнический университет Петра Великого
- Университет ИТМО
- Группа компаний «Марвел»
- АО «Институт инфотелекоммуникаций»
- АО «Концерн «НПО «Аврора»
- АО «Научно-исследовательский институт программных средств»
- АО «Научно-производственное объединение «Импульс»
- АО «Научно-технический центр биоинформатики и телемедицины «Фрактал»
- АО «НИИ «Масштаб»
- АО «Центр компьютерных разработок»
- ЗАО «Институт телекоммуникаций»
- ООО «Геонавигатор»
- ООО «Лаборатория инфокоммуникационных сетей»
- ООО «НеоБИТ»
- ПАО «ИНТЕЛТЕХ»
- Партнерство для развития информационного общества на Северо-Западе России
- Санкт-Петербургская инженерная академия
- Санкт-Петербургское отделение Академии инженерных наук им. А.М. Прохорова
- Санкт-Петербургское отделение Академии информатизации образования
- Санкт-Петербургское отделение Международной академии информатизации



## КООРДИНАЦИОННЫЙ СОВЕТ КОНФЕРЕНЦИИ

|                               |                                                                                                                                                                                                         |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Беглов Александр Дмитриевич   | Губернатор Санкт-Петербурга                                                                                                                                                                             |
| Бельский Александр Николаевич | Председатель Законодательного собрания Санкт-Петербурга                                                                                                                                                 |
| Дрозденко Александр Юрьевич   | Губернатор Ленинградской области                                                                                                                                                                        |
| Фальков Валерий Николаевич    | Министр науки и высшего образования Российской Федерации                                                                                                                                                |
| Шадаев Максуд Игоревич        | Министр цифрового развития, связи и массовых коммуникаций Российской Федерации                                                                                                                          |
| Красников Геннадий Яковлевич  | Президент Российской академии наук, академик Российской академии наук                                                                                                                                   |
| Рудской Андрей Иванович       | Президент Санкт-Петербургского отделения Российской академии наук, ректор Санкт-Петербургского политехнического университета Петра Великого, академик Российской академии наук                          |
| Радченко Валерий Анатольевич  | Президент Ассоциации промышленных предприятий Санкт-Петербурга                                                                                                                                          |
| Железков Сергей Валерьевич    | Руководитель Управления Федеральной службы технического и экспортного контроля по Северо-Западному федеральному округу                                                                                  |
| Шерстюк Владислав Петрович    | Президент Национальной ассоциации международной информационной безопасности, член-корреспондент Академии криптографии Российской Федерации, советник Секретаря Совета Безопасности Российской Федерации |

## ПРЕЗИДИУМ КОНФЕРЕНЦИИ

|                                   |                                                                                                                                                                                                                                                                              |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Советов Борис Яковлевич           | Председатель Президиума конференции, председатель Программного комитета, сопредседатель Научного совета по информатизации Санкт-Петербурга, академик Российской академии образования                                                                                         |
| Белов Евгений Борисович           | Председатель Федерального УМО ВО в области информационной безопасности, заместитель начальника института криптографии, связи и информатики «Академии ФСБ России»                                                                                                             |
| Ильин Николай Иванович            | Заместитель начальника Управления информационных систем Службы специальной связи и информации ФСО России                                                                                                                                                                     |
| Омельницкий Владимир Владимирович | Вице-губернатор Санкт-Петербурга                                                                                                                                                                                                                                             |
| Максимов Андрей Станиславович     | Председатель Комитета по науке и высшей школе Санкт-Петербурга                                                                                                                                                                                                               |
| Смирнова Юлия Леонидовна          | Председатель Комитета по информатизации и связи Санкт-Петербурга                                                                                                                                                                                                             |
| Панкевич Виктор Николаевич        | Заместитель руководителя Администрации Губернатора Санкт-Петербурга – Начальник Управления делами                                                                                                                                                                            |
| Пешехонов Владимир Григорьевич    | Научный руководитель ГНЦ «Центральный научно-исследовательский институт «Электроприбор», заместитель председателя Санкт-Петербургского отделения Российской академии наук, академик Российской академии наук                                                                 |
| Ронжин Андрей Леонидович          | Директор Санкт-Петербургского Федерального исследовательского центра Российской академии наук, профессор РАН                                                                                                                                                                 |
| Осипов Василий Юрьевич            | Председатель Организационного комитета, директор СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук                                                                                                                                |
| Смирнов Анатолий Иванович         | Президент Национального института исследований глобальной безопасности, профессор Московского государственного института международных отношений (университета) Министерства иностранных дел Российской Федерации, председатель Отделения РАЕН «Информационная глобализация» |

|                                  |                                                                                                                                                                                                                                                                                                  |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Стрельцов Анатолий Александрович | Вице-президент Национальной ассоциации международной информационной безопасности, профессор, ведущий научный сотрудник факультета вычислительной математики Московского государственного университета им. М.В. Ломоносова, действительный государственный советник Российской Федерации 3 класса |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## **ОРГАНИЗАЦИОННЫЙ КОМИТЕТ КОНФЕРЕНЦИИ**

### **Председатель Организационного Комитета**

|                        |                                                                                                       |
|------------------------|-------------------------------------------------------------------------------------------------------|
| Осипов Василий Юрьевич | Директор СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук |
|------------------------|-------------------------------------------------------------------------------------------------------|

### **Заместитель председателя Организационного Комитета**

|                             |                                                                                                                                                  |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Жигadlo Валентин Эдуардович | Заместитель генерального директора ЗАО «Институт телекоммуникаций», президент Санкт-Петербургского отделения Академии информатизации образования |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|

### **Члены Организационного Комитета**

|                                  |                                                                                                                                                                                                                         |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Алексеев Анатолий Владимирович   | Исполнительный директор Института автоматизации процессов борьбы за живучесть корабля, судна, профессор кафедры судовой автоматики и измерений Санкт-Петербургского государственного морского технического университета |
| Антохина Юлия Анатольевна        | Ректор Санкт-Петербургского государственного университета аэрокосмического приборостроения                                                                                                                              |
| Барышников Сергей Олегович       | Ректор Государственного университета морского и речного флота имени адмирала С.О. Макарова                                                                                                                              |
| Басков Вячеслав Дмитриевич       | Генеральный директор ООО «НеоБИТ»                                                                                                                                                                                       |
| Блажис Анатолий Константинович   | Директор АО «Научно-технический центр биоинформатики и телемедицины «Фрактал»                                                                                                                                           |
| Бобрович Владимир Юрьевич        | Директор по стратегическому и инновационному развитию АО «Концерн «НПО «Аврора»                                                                                                                                         |
| Богданов Владимир Николаевич     | Директор АО «ЦентрИнформ», лауреат Государственной премии Российской Федерации в области науки и техники                                                                                                                |
| Борисов Николай Валентинович     | Заведующий кафедрой Санкт-Петербургского государственного университета                                                                                                                                                  |
| Васильев Владимир Николаевич     | Ректор Университета ИТМО, член-корреспондент Российской академии образования, член-корреспондент Российской академии наук                                                                                               |
| Гаценко Олег Юрьевич             | Генеральный директор АО «Научно-исследовательский институт программных средств»                                                                                                                                         |
| Гирдин Сергей Алексеевич         | Президент Группы компаний «Марвел»                                                                                                                                                                                      |
| Григорьев Владимир Александрович | Генеральный директор ООО «Лаборатория инфокоммуникационных сетей», президент Санкт-Петербургского отделения Общероссийской общественной организации «Академия инженерных наук им. А.М. Прохорова»                       |
| Датаяшева Камила Камильевна      | Директор Дома ученых им. М. Горького, почетный работник высшего профессионального образования Российской Федерации, почетный член Российской академии художеств                                                         |
| Демидов Алексей Вячеславович     | Ректор Санкт-Петербургского государственного университета промышленных технологий и дизайна, вице-президент Российского союза ректоров, председатель Совета ректоров вузов Санкт-Петербурга и Ленинградской области     |
| Демин Евгений Николаевич         | Начальник управления популяризации науки Санкт-Петербургского отделения Российской академии наук                                                                                                                        |
| Жданов Сергей Николаевич         | Советник генерального директора АО ВТБ Девелопмент по внешним связям                                                                                                                                                    |



|                               |                                                                                                                                                                                                                                                |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Жигадло Валентин Эдуардович   | Заместитель генерального директора ЗАО «Институт телекоммуникаций», президент Санкт-Петербургского отделения Академии информатизации образования                                                                                               |
| Зайцева Александра Алексеевна | Ученый секретарь Санкт-Петербургского Федерального исследовательского центра Российской академии наук                                                                                                                                          |
| Захаров Юрий Никитич          | Первый заместитель директора СПб ГКУ «Санкт-Петербургский информационно-аналитический центр»                                                                                                                                                   |
| Зегжда Дмитрий Петрович       | Директор Института компьютерных наук и кибербезопасности Санкт-Петербургского политехнического университета Петра Великого, член-корреспондент Российской академии наук                                                                        |
| Ипатов Олег Сергеевич         | Директор Центра научно-технологического партнерства и целевой подготовки Санкт-Петербургского политехнического университета Петра Великого                                                                                                     |
| Касаткин Виктор Викторович    | Ученый секретарь Научного совета по информатизации Санкт-Петербурга, заместитель начальника отдела аспирантуры Санкт-Петербургского Федерального исследовательского центра Российской академии наук                                            |
| Кефели Игорь Федорович        | Директор проекта «Когнитивная безопасность» Северо-Западного института управления Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, заслуженный работник высшей школы Российской Федерации |
| Корниенко Анатолий Адамович   | Профессор кафедры информатики и информационной безопасности Петербургского государственного университета путей сообщения Императора Александра I                                                                                               |
| Крупцов Сергей Владимирович   | Первый заместитель генерального директора АО «Центр компьютерных разработок»                                                                                                                                                                   |
| Кузичкин Александр Васильевич | Главный научный сотрудник АО «НИИ телевидения», заслуженный связист Российской Федерации, заслуженный деятель науки Российской Федерации                                                                                                       |
| Кузьмин Юрий Григорьевич      | Ученый секретарь Санкт-Петербургского Общества информатики, вычислительной техники, систем связи и управления                                                                                                                                  |
| Кулешов Игорь Александрович   | Заместитель генерального директора по научной работе ПАО «ИНТЕЛТЕХ»                                                                                                                                                                            |
| Куприянов Михаил Степанович   | руководитель перспективных проектов Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), заслуженный работник высшей школы Российской Федерации                                           |
| Кучерявый Михаил Михайлович   | Советник генерального директора АО «Корпорация Московский институт теплотехники» Государственной корпорации «Роскосмос», Государственный советник Российской Федерации 1 класса                                                                |
| Максимцев Игорь Анатольевич   | Ректор Санкт-Петербургского государственного экономического университета                                                                                                                                                                       |
| Маркова Виктория Сергеевна    | Начальник отдела научных конкурсов и мероприятий Санкт-Петербургского отделения Российской академии наук.                                                                                                                                      |
| Михайлов Николай Семенович    | Заместитель генерального директора по информационным технологиям и стратегии развития АО «Равенство»                                                                                                                                           |
| Михайлова Анна Сергеевна      | Заместитель директора Санкт-Петербургского Общества информатики, вычислительной техники, систем связи и управления по связям с общественностью                                                                                                 |
| Михеев Валерий Леонидович     | Ректор Российского государственного гидрометеорологического университета                                                                                                                                                                       |
| Молдовян Александр Андреевич  | Главный научный сотрудник лаборатории кибербезопасности и постквантовых криптосистем СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук                                                              |
| Николашин Юрий Львович        | Генеральный директор ПАО «ИНТЕЛТЕХ», генеральный конструктор системы управления ВМФ                                                                                                                                                            |

|                                |                                                                                                                                                                                                                    |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Никулин Евгений Николаевич     | Ректор Санкт-Петербургского института экономики и бизнеса, профессор Балтийского государственного технического университета «ВОЕНМЕХ» им. Д.Ф. Устинова                                                            |
| Нырков Анатолий Павлович       | Заведующий кафедрой комплексного обеспечения информационной безопасности Государственного университета морского и речного флота имени адмирала С.О. Макарова                                                       |
| Оводенко Анатолий Аркадьевич   | Президент Санкт-Петербургского государственного университета аэрокосмического приборостроения                                                                                                                      |
| Присяжнюк Сергей Прокофьевич   | Научный руководитель ЗАО «Институт телекоммуникаций», профессор Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича                                                   |
| Пролетарский Андрей Викторович | Декан факультета «Информатика и системы управления» Московского государственного технического университета им. Н.Э. Баумана, председатель Федерального УМО по УГСН 09.00.00 «Информатика и вычислительная техника» |
| Пухов Геннадий Георгиевич      | Директор ООО «Геонавигатор», заместитель сопредседателя Научного совета по информатизации Санкт-Петербурга                                                                                                         |
| Силла Евгений Петрович         | Ученый секретарь СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук                                                                                                      |
| Соколов Сергей Сергеевич       | Первый проректор, профессор кафедры комплексного обеспечения информационной безопасности Государственного университета морского и речного флота имени адмирала С.О. Макарова                                       |
| Строганов Дмитрий Викторович   | Профессора кафедры АСУ Московского автомобильно-дорожного государственного технического университета (МАДИ), эксперт РАН, председатель Учебно-методического совета 09.00.02 «Информационные системы и технологии»  |
| Тихомиров Сергей Григорьевич   | Генеральный директор АО «Центр компьютерных разработок»                                                                                                                                                            |
| Туричин Глеб Андреевич         | Ректор Санкт-Петербургского государственного морского технического университета                                                                                                                                    |
| Улесов Денис Васильевич        | Исполняющий обязанности директора СПб ГКУ «Санкт-Петербургский информационно-аналитический центр»                                                                                                                  |
| Чугунов Андрей Владимирович    | Директор Центра технологий электронного правительства Института дизайна и урбанистики Университета ИТМО, генеральный директор НП ПРИОР Северо-Запад                                                                |
| Шелудько Виктор Николаевич     | Ректор Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина)                                                                                                    |
| Шерстюк Юрий Михайлович        | Генеральный директор АО «Институт инфотелекоммуникаций»                                                                                                                                                            |
| Шилов Константин Юрьевич       | Генеральный директор АО «Концерн «НПО «Аврора»                                                                                                                                                                     |

## **ПРОГРАММНЫЙ КОМИТЕТ КОНФЕРЕНЦИИ**

### **Председатель Программного Комитета**

|                         |                                                                                                                                                                                                                                                                                                                                  |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Советов Борис Яковлевич | Сопредседатель Научного совета по информатизации Санкт-Петербурга, заслуженный профессор Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), академик Российской академии образования, заслуженный деятель науки и техники Российской Федерации, д-р техн. наук, профессор |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### **Заместитель председателя Программного Комитета**

|                             |                                                                                                       |
|-----------------------------|-------------------------------------------------------------------------------------------------------|
| Никонов Игорь Александрович | Первый заместитель председателя Комитета по информатизации и связи Санкт-Петербурга, канд. техн. наук |
|-----------------------------|-------------------------------------------------------------------------------------------------------|

### **Члены Программного комитета – руководители и секретари секций**

|                                |                                                                                                                                                                                                                                            |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Абрамов Максим Викторович      | Ведущий научный сотрудник, руководитель лаборатории прикладного искусственного интеллекта СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук, канд. техн. наук                                   |
| Алексеев Анатолий Владимирович | Профессор кафедры судовой автоматики и измерений Санкт-Петербургского государственного морского технического университета, директор НП «Институт автоматизации процессов борьбы за живучесть корабля, судна, д-р техн. наук, профессор     |
| Беззатеев Сергей Валентинович  | Заведующий кафедрой информационной безопасности Санкт-Петербургского государственного университета аэрокосмического приборостроения, профессор факультета безопасности информационных технологий Университета ИТМО, д-р техн. наук, доцент |
| Бударный Глеб Сергеевич        | Старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича                                                                                     |
| Бурлов Вячеслав Георгиевич     | И.о. заведующего кафедрой информационных технологий и систем безопасности Российского государственного гидрометеорологического университета, д-р техн. наук, профессор                                                                     |
| Верзун Наталья Аркадьевна      | Доцент кафедры информационных систем и технологий Санкт-Петербургского государственного экономического университета, канд. техн. наук, доцент                                                                                              |
| Виноградов Александр Андреевич | Главный эксперт АО «НПО «Импульс»                                                                                                                                                                                                          |
| Горбунова Ирина Борисовна      | Руководитель Научно-методической лаборатории «Музыкально-компьютерные технологии», профессор кафедры цифрового образования Российского государственного педагогического университета им. А. И. Герцена, д-р. пед. наук, профессор          |
| Волкова Алла Александровна     | Лаборант кафедры судовой автоматики и измерений Санкт-Петербургского государственного морского технического университета                                                                                                                   |
| Жернова Ксения Николаевна      | Старший научный сотрудник лаборатории проблем компьютерной безопасности СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук, канд. техн. наук                                                     |
| Жигадло Валентин Эдуардович    | Заместитель генерального директора ЗАО «Институт телекоммуникаций», президент Санкт-Петербургского отделения Академии информатизации образования, д-р техн. наук, доцент                                                                   |
| Заколдаев Данил Анатольевич    | Декан факультета безопасности информационных технологий Университета ИТМО, канд. техн. наук, доцент                                                                                                                                        |
| Захаров Юрий Никитич           | Советник директора Санкт-Петербургского информационно-аналитического центра, канд. техн. наук, профессор                                                                                                                                   |
| Зикратов Игорь Алексеевич      | Декан факультета кибербезопасности, профессор кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, д-р техн. наук, профессор                        |
| Иващенко Анастасия Олеговна    | Научный сотрудник лаборатории прикладного искусственного интеллекта СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук                                                                           |
| Игумнов Владимир Вячеславович  | Советник генерального директора АО «НПО «Импульс», профессор Академии военных наук, канд. техн. наук                                                                                                                                       |
| Искандеров Юрий Марсович       | Главный научный сотрудник – руководитель лаборатории интеллектуальных систем СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук, д-р техн. наук, профессор                                       |

|                               |                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Истомин Евгений Петрович      | Директор института геоинформационных систем и технологий Российского государственного гидрометеорологического университета, д-р техн. наук, профессор, почетный работник науки и высоких технологий Российской Федерации, д-р техн. наук, профессор                                                                               |
| Кефели Игорь Федорович        | Директор проекта «Когнитивная безопасность» Северо-Западного института управления Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, заслуженный работник высшей школы Российской Федерации, д-р филос. наук, профессор                                                        |
| Колбанёв Михаил Олегович      | Профессор Санкт-Петербургского государственного экономического университета, д-р техн. наук, профессор                                                                                                                                                                                                                            |
| Коржук Виктория Михайловна    | Доцент факультета безопасности информационных технологий Университета ИТМО, канд. техн. наук                                                                                                                                                                                                                                      |
| Коротков Виталий Валерьевич   | Доцент кафедры комплексного обеспечения информационной безопасности Государственного университета морского и речного флота имени адмирала С.О. Макарова, канд. техн. наук, доцент                                                                                                                                                 |
| Коршунов Игорь Львович        | Заведующий кафедрой информационных систем и технологий Санкт-Петербургского государственного экономического университета, канд. техн. наук, доцент                                                                                                                                                                                |
| Косолапов Алексей Дмитриевич  | Заведующий кафедрой математических, естественнонаучных и общеприкладных дисциплин Военной ордена Жукова академии войск национальной гвардии Российской Федерации, канд. пед. наук, доцент                                                                                                                                         |
| Котенко Игорь Витальевич      | Главный научный сотрудник, заведующий лабораторией проблем компьютерной безопасности СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук, заслуженный деятель науки Российской Федерации, д-р техн. наук, профессор                                                                      |
| Красов Андрей Владимирович    | Заведующий кафедрой защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, канд. техн. наук, доцент, заслуженный работник высшей школы Российской Федерации, почетный работник высшего образования Российской Федерации, академик международной академии связи |
| Ласкин Михаил Борисович       | Главный научный сотрудник лаборатории интеллектуальных систем СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук, д-р экон. наук, канд. физ.-мат. наук, доцент                                                                                                                          |
| Литвинов Владислав Леонидович | Заведующий кафедрой информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, канд. техн. наук, доцент                                                                                                                                                  |
| Мельник Галина Сергеевна      | Профессор кафедры цифровых медиакоммуникаций Высшей школы журналистики и массовых коммуникаций Санкт-Петербургского государственного университета, д-р полит. наук, профессор                                                                                                                                                     |
| Микадзе Сергей Юрьевич        | Директор Департамента комплексной безопасности Санкт-Петербургского государственного экономического университета, канд. экон. наук                                                                                                                                                                                                |
| Михальчук Андрей Васильевич   | Доцент кафедры судовой автоматики и измерений Санкт-Петербургского государственного морского технического университета, канд. техн. наук.                                                                                                                                                                                         |
| Молдовян Дмитрий Николаевич   | Доцент кафедры «Информационные системы» Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), канд. техн. наук.                                                                                                                                                               |
| Молдойн Николай Андреевич     | Профессор кафедры «Информационные системы» Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), д-р техн. наук, профессор                                                                                                                                                    |

|                                 |                                                                                                                                                                                                                                        |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Мороз Николай Васильевич        | Заместитель директора ООО «Геонавигатор»                                                                                                                                                                                               |
| Новикова Тамара Алексеевна      | Информационный менеджер Центра технологий электронного правительства Института дизайна и урбанистики Университета ИТМО, магистрант Института дизайна и урбанистики Университета ИТМО                                                   |
| Нырков Анатолий Павлович        | Заведующий кафедрой комплексного обеспечения информационной безопасности Государственного университета морского и речного флота имени адмирала С.О. Макарова, д-р техн. наук, профессор                                                |
| Осипов Василий Юрьевич          | Директор СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук, д-р техн. наук, профессор                                                                                                       |
| Паращук Игорь Борисович         | Профессор кафедры автоматизированных систем специального назначения Военной академии связи им. С.М. Буденного, заслуженный изобретатель Российской Федерации, д-р техн. наук, профессор                                                |
| Петриева Оксана Владимировна    | Доцент кафедры математических, естественнонаучных и общеприкладных дисциплин Военной ордена Жукова академии войск национальной гвардии Российской Федерации, канд. тех. наук, доцент                                                   |
| Плебанек Ольга Васильевна       | Заведующий. кафедрой социально-гуманитарных дисциплин Университета при МПА ЕврАзЭС, д-р филос. наук, доцент                                                                                                                            |
| Поляничева Анна Валерьевна      | Старший преподаватель кафедры информационной безопасности компьютерных сетей Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича                                                          |
| Примак Анна Викторовна          | Преподаватель кафедры судовой автоматики и измерений Санкт-Петербургского государственного морского технического университета                                                                                                          |
| Примакин Алексей Иванович       | Профессор кафедры математических, естественнонаучных и общеприкладных дисциплин Военной ордена Жукова академии войск национальной гвардии Российской Федерации, д-р техн. наук, профессор                                              |
| Пухов Геннадий Георгиевич       | Директор ООО «Геонавигатор», заместитель сопредседателя Научного совета по информатизации Санкт-Петербурга, канд. техн. наук, профессор                                                                                                |
| Родионов Дмитрий Сергеевич      | Директор обсерватории института физики Российского государственного педагогического университета им. А. И. Герцена; канд. физ-мат. наук                                                                                                |
| Саенко Игорь Борисович          | Главный научный сотрудник лаборатории проблем компьютерной безопасности СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук, д-р техн. наук, профессор                                        |
| Саяркин Леонид Андреевич        | Адъюнкт Военной академии связи им. С.М. Буденного                                                                                                                                                                                      |
| Сергеев Виталий Владимирович    | Главный ученый секретарь Санкт-Петербургского отделения РАН, первый проректор Санкт-Петербургского политехнического университета Петра Великого, член-корреспондент Российской академии наук, профессор РАН, д-р техн. наук, профессор |
| Согонов Сергей Александрович    | Заведующий кафедрой судовой автоматики и измерений Санкт-Петербургского государственного морского технического университета, канд. техн. наук, доцент                                                                                  |
| Соколов Сергей Сергеевич        | Первый проректор, профессор кафедры комплексного обеспечения информационной безопасности Государственного университета морского и речного флота имени адмирала С.О. Макарова, д-р техн. наук, профессор                                |
| Татарникова Татьяна Михайловна, | Директор Института информационных технологий и программирования Санкт-Петербургского государственного университета аэрокосмического приборостроения, д-р техн. наук, профессор                                                         |
| Устинов Игорь Анатольевич       | Советник генерального директора АО «НПО «Импульс», канд. техн. наук, член-корреспондент Академии военных наук, канд. техн. наук                                                                                                        |

|                                    |                                                                                                                                                                                                                                                                                         |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Утюганов Алексей Анатольевич       | Заместитель начальника Военной ордена Жукова академии войск национальной гвардии Российской Федерации по научной работе – начальник научно-исследовательского центра, полковник, д-р психол. наук, доцент                                                                               |
| Ушаков Игорь Александрович         | Доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, кандидат технических наук, доцент                                                                                                              |
| Филатова Ольга Георгиевна          | Доцент кафедры связей с общественностью в политике и государственном управлении Санкт-Петербургского государственного университета, ведущий научный сотрудник Центра технологий электронного правительства Института дизайна и урбанистики Университета ИТМО, канд. филос. наук, доцент |
| Цехановский Владислав Владимирович | Профессор, заместитель заведующего кафедрой «Информационные системы» Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), канд. техн. наук, доцент                                                                                 |
| Чугунов Андрей Владимирович        | Директор Центра технологий электронного правительства Института дизайна и урбанистики Университета ИТМО, генеральный директор НП ПРИОР Северо-Запад, канд. политич. наук, доцент                                                                                                        |
| Штеренберг Станислав Игоревич      | Доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, кандидат технических наук                                                                                                                      |

#### **Ученый секретарь Конференции**

|                            |                                                                                                                                                                                                                               |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Касаткин Виктор Викторович | Ученый секретарь Научного совета по информатизации Санкт-Петербурга, заместитель начальника отдела аспирантуры Санкт-Петербургского Федерального исследовательского центра Российской академии наук, канд. техн. наук, доцент |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



## ГОСУДАРСТВЕННАЯ ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕГИОНОВ РОССИИ

УДК 004.9:351.9

### БАРЬЕРЫ ВНЕДРЕНИЯ ЦИФРОВЫХ СЕРВИСОВ В ГОССЕКТОРЕ

**Денисов Максим Васильевич**

Северо-Западный институт управления - филиал РАНХиГС

Средний пр-т, д. 57/43, Санкт-Петербург, 199178, Россия

e-mail: denisov-mv@ranepa.ru

**Аннотация.** В докладе рассмотрены типовые ошибки и риски, связанные с внедрением и реализацией государственных информационных систем. В явном виде выделены нерешённые проблемы, которые воспроизводятся при внедрении цифровых сервисов в госсекторе. В ходе исследования проведён анализ возникающих барьеров при внедрении государственных информационных систем (ГИС) на разных качественных уровнях, а также приведены возможные способы их преодоления за счёт опоры на имеющиеся ресурсы. Данным исследованием мы хотим показать участникам процесса, какие существуют возможные ходы для обхода барьеров и решения проблем на имеющихся ресурсах без привлечения дополнительных средств и т.д.

**Ключевые слова:** ошибки цифровизации; риски цифровой трансформации; проблемы внедрения ГИС; ресурсный подход в ГИС.

### BARRIERS TO THE INTRODUCTION OF DIGITAL SERVICES IN THE PUBLIC SECTOR

**Denisov Maxim**

North-West Institute of Management - branch of RANEPa

57/43, Sredny Av, St. Petersburg, 199178, Russia

e-mail: denisov-mv@ranepa.ru

**Abstract.** The report examines typical errors and risks associated with the introduction and implementation of government information systems (GIS). The unresolved problems that are reproduced in the implementation of digital services in the public sector are explicitly highlighted. The study analyzes the barriers that arise in the implementation of GIS at different qualitative levels, and also provides possible ways to overcome them by relying on available resources. With this study, we want to show the participants in the process what possible moves exist to circumvent barriers and solve problems using available resources without attracting additional funds, etc.

**Keywords:** digitalization errors; digital transformation risks; GIS implementation problems; resource approach in GIS.

В ходе исследования проведён анализ возникающих барьеров при внедрении государственных информационных систем (ГИС) на разных качественных уровнях, а также приведены возможные способы их преодоления за счёт опоры на имеющиеся ресурсы. К типовым ошибкам и рискам внедрения ГИС и цифровых сервисов относятся:

1. Неучёт ограничений нарастающей цифровой инфраструктуры ГИС, которую государству всё сложнее обслуживать [1].
2. Переключение государства на решение более актуальных задач (пандемия, СВО) в ответ на внешние вызовы.
3. Вместо решения задач по обеспечению цифрового суверенитета и безопасности критической информационной инфраструктуры (КИИ): (а) негласный запрет на обратную связь по ошибкам и проблемам [2]; (б) замалчивание проблемы под видом закрытых данных; (в) подмена цели обеспечения безопасности КИИ так называемым импортозамещением; (г) игнорирование «стоп-факторов» при создании информационных систем; риски vendor log in — постановка в зависимость, в т.ч. от отечественного вендора.
4. Задача по цифровизации функционально решается, а пользовательская задача не решается: (а) неучёт барьеров пользователя / сотрудника / руководителя; (б) сохранение / увеличение рутинных / неоптимальных действий пользователя вместо их автоматизации; (в) невозможность выполнения действий пользователем в соответствии требованиями нормативно-правовых актов (НПА).
5. Создание избыточной / неоптимальной ИКТ-инфраструктуры, вызывающей потери, вместо оптимального переиспользования тех мощностей / данных, которые уже имеются: (а) игнорирование ресурсов инфраструктуры, мощностей, команд, которые уже работают: (а) непереиспользование сервисов / систем / инфраструктуры ГИС ведёт к её неэффективной эксплуатации [3]; (б) «цифровой зоопарк» приводит к

устойчивому нарушению работы, когда сотрудники не способны продуктивно выполнять заданные функции; (в) провал проекта системной интеграции ГИС.

Выделим нерешённые проблемы внедрения ГИС и цифровых сервисов:

- проблема межведомственного взаимодействия, когда органам исполнительной власти в буквальном смысле между собой не договориться;
- отсутствие полномочий у органов исполнительной власти, необходимых для реализации цифрового сервиса;
- административные барьеры легализации ГИС;
- противоречия и конфликты с подрядчиками.

Анализ прецедентов позволил выделить три качественных уровня барьеров внедрения ГИС и способов их преодоления.

#### *А. Уровень «Цели / интересы»*

В основании барьеров данного уровня лежат противоречия и конфликтные ситуации из-за наличия разных целей / интересов участников, способные выступить преградой для создания ГИС. Неурегулированность конфликтов и противоречий порождают риски, которые могут возникать:

- внутри органа власти, учреждения, например, когда руководитель не поддерживает проект;
- между разными органами власти, например, когда нижестоящий ОИВ блокирует цифровой сервис, чтобы вышестоящий ОИВ не имел доступа к чувствительной информации;
- между органом власти и бизнес-структурами, например, когда государственный проект противоречит интересам монополиста или крупного рыночного игрока.

В качестве возможных стратегий обхода данных барьеров с опорой на существующие ресурсы, которые уже есть в системе, можно предложить следующие:

- поддержка первым лицом города / региона внедрения и желание применять возможности, которые дают новые технологии;
- приглашение в проект компанию разработчика, которая только начинает свою деятельность;
- назначение единственного исполнителя для снижения рисков реализации государственного проекта, требующего значительных изменений [2].

#### *В. Уровень «Межведомственное и межуровневое взаимодействие»*

Проблемы на данном уровне могут порождать следующие барьеры для реализации ГИС:

- подмена создания единой ГИС на уровне города дублированием ИТ-инфраструктуры подведомственных учреждений.
- вместо синхронизации ГИС на уровне региона порождение т.н. «ведомственных колодцев».

В качестве возможных стратегий обхода барьеров межведомственного и межуровневого взаимодействия можно выделить следующие:

- длительная подготовка к сложно реализуемому проекту для отсека ошибок и рисков, в том числе: а) привлечение лучших экспертов в отсутствие нужных компетенций; б) выполнение функций и работ за тех, кто закономерно от них будет отказываться; в) неожиданное благодарности за полученный результат;
- выступить «тайным покупателем» госуслуг для сбора данных из объективной реальности, поскольку если данные искажены, это может быть критичным для реализации проекта.

#### *С. Уровень «Создание / применение ГИС»*

Цифровой сервис может столкнуться с проблемами реализации из-за запретов и ограничений следующего характера:

- отсутствие полностью / частично полномочий у органов власти, например, для создания ГИС, которая может быть масштабируема на территории других субъектов;
- невозможность гибко переключиться на разработку более перспективного цифрового сервиса вместо устаревшего, который вынуждены эксплуатировать.

Выделим возможные стратегии обхода барьеров, связанных с отсутствием полномочий и наличия противоречивых требований к инструментам для финансирования ГИС:

- использование функции / роли Заказчика как ресурса для входа в новую область деятельности и отбора лучших практик;
  - отказ от субсидии для финансирования ГИС, если её требования непрозрачны и противоречивы;
  - обход ограничений бюджетного цикла во времени на ресурсе легально предоставленного ПО;
- Проблема применения ГИС и цифровых сервисов может быть вызвана следующими барьерами:
- привычка руководителей принимать решения не на основе данных;
  - отказ сотрудников использовать цифровой сервис в своей деятельности;
  - игнорирование функций главного верификатора, медиатора процесса создания и распространения открытых данных для разработчиков.

В качестве возможных стратегий обхода данных барьеров можно предложить следующие:

- постановка задачи по легализации принятия решений на основе данных;
- установление запрета на привычные «аналоговые», но не оптимальные действия в ГИС;
- выявление (по сути, «бесплатных») ресурсов и их преобразование в решение задач города / региона;



— использование ситуации, в контексте которой переход на новые цифровые продукты будет произведён естественным образом.

Исследование построено на обобщении массива прецедентов, включающих более 50 оригинальных примеров из базы данных автора.

#### СПИСОК ЛИТЕРАТУРЫ

1. Чернышенко Д.Н. Доклад на тему: «Использование единой платформы «ГосТех»» / 23 октября 2021 года в координационном центре Правительства состоялась первая официальная презентация платформы «Гостех» Опубликовано на Видеоканале «Tadviser» URL: <https://youtu.be/hEnKS18kj-0?t=251> (дата обращения: 19.05.2025).
2. Что не так с цифровизацией госсектора? Подкаст Tadviser с Ю.Н. Даценко URL: <https://rutube.ru/video/508c319a4873265173190f832d5b55cb/?t=a> (дата обращения: 19.05.2025).
3. Бюллетень Счетной палаты № 8 (297) 2022 г. «Государственные информационные системы». URL: <https://ach.gov.ru/statements/bulletin-sp-8-2022> (дата обращения 19.07.2025).

УДК 070.1; 304.4

### СОЦИОКУЛЬТУРНЫЕ ЦЕННОСТИ ВОЕННОЙ ЖУРНАЛИСТИКИ КАК АКСИОЛОГИЧЕСКИЙ ИНСТРУМЕНТ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Ерофеева Ирина Викторовна<sup>1</sup>, Михалева Людмила Игоревна<sup>2</sup>

<sup>1</sup>Забайкальский государственный университет  
Александрово-Заводская, 30, Чита, 672039, Россия

<sup>2</sup>Волгоградский государственный университет  
Университетский проспект, д. 100, Волгоград, 400062, Россия  
e-mail: : irina-jour@yandex.ru, mihaleva2004@mail.ru

**Аннотация.** Представлены результаты лингвокультурологического анализа медиадискурса военных журналистов, выделены доминирующие социокультурные ценности, которые являются не только когнитивными конструктами обработки фактуры языковой личностью автора, но и способны поддерживать состояние защищенности национальных интересов России.

**Ключевые слова:** военная журналистика; национальная безопасность; языковая личность журналиста; медиадискурс; национальная картина мира; социокультурные ценности.

### SOCIOCULTURAL VALUES OF MILITARY JOURNALISM AS AN AXIOLOGICAL INSTRUMENT OF NATIONAL SECURITY

Erofeeva Irina<sup>1</sup>, Lyudmila Igorevna<sup>2</sup>

<sup>1</sup>Transbaikalian State University  
30 Aleksandro-Zavodskaya St., Chita, 672039, Russia

<sup>2</sup>Volgograd State University  
100 Universitetsky Prospekt, Volgograd, 400062, Russia  
e-mail: irina-jour@yandex.ru, mihaleva2004@mail.ru

**Abstract.** The article presents the results of the linguacultural analysis of the media discourse of military journalists, highlights the dominant sociocultural values, which are not only cognitive constructs of processing the texture by the linguistic personality of the author, but are also capable of maintaining the state of protection of Russia's national interests.

**Keywords:** military journalism; national security; journalist's linguistic personality; media discourse; national picture of the world; socio-cultural values.

Доминирующие информационные потоки российских массмедиа заполнены материалами о специальной военной операции, в которых присутствуют темы, крайне важные для большинства жителей страны. Поэтому сегодня работа военного журналиста связана не только с информированием и документализацией событий, умением работать в сложных и потенциально опасных условиях, но и со способностью понимать первопричину и глубину происходящего, видеть вектор развития национальной истории, обеспечивая информационную и национальную безопасность страны.

Результаты предлагаемого исследования опираются на проведенный нами лингвокультурологический анализ более 250 материалов о специальной военной операции ряда журналистов (Дмитрий Григорьев, Александр Коц, Дмитрий Стешин, Дарья Асламова, Юлия Андриенко), которые были опубликованы в интернет-изданиях «Аргументы и факты», Комсомольская правда, Правда.Ру. (Pravda.RU) с 2022 по 2024 гг.

В процессе работы были задействованы поисковые системы Яндекс и Гугл, специализированные рубрики военкоров и подборки «Комсомольской правды» (<https://www.kp.ru/daily/theme/16422/>) и «АиФ» (<https://perm.aif.ru/opinion/author/21326?ysclid=m1hntbq3o0398605518>).

В рамках исследования медиадискурс мы рассматриваем как пространство аккумуляции и передачи социокультурных ценностей от автора к потребителю, как формат накопления и трансляции культурных норм и ценностей российского общества [4]. Человек, будучи социальным существом, предпочитает жить в

гармонии с базовыми фундаментальными ценностями, соотносёнными со знаковыми реалиями его культуры и объединяющими основные представления людей относительно целей и норм своего существования [3, с. 3].

Как отмечает Г. П. Выжлецов, ценности позволяют увидеть культуру народа и общества изнутри, из глубин социальной и индивидуальной жизни [2]. По мнению Момджян К. Х., они демонстрируют критерии мотивационного выбора человека [7].

Медиаэксперт Л. В. Баева пишет о ценностях как о необходимых инструментах жизни личности в выражении «внутренней свободы и возможности субъективации внешнего бытия» [1, с. 8]. По мнению исследователя, ценность проявляется в трёх компонентах жизни человека: значимость, смысл и переживание. Ценность становится реальностью, когда она человеком ощущается, осознаётся и осмысливается интуитивно и интеллектуально.

Социокультурные ценности выступают как признанные обществом ориентиры, некие устоявшиеся общепринятые убеждения, воплощающие традиционный уклад жизни. Они формируются вековым развитием народа, несут в себе коллективную память поколений и воспроизводятся в процессе социализации и в повседневной жизни, передаются от поколения к поколению, определяя основы общественного жизнеустройства [7]. Эти ценности имеют объединяющий характер, связывая культурные устои прошлого с реалиями современности. Утрата национальных ориентиров ведет к деградации культурной идентичности, превращению нации в безликое общество, лишённое корней, традиций и исторических воспоминаний, — крайне уязвимое в условиях современной глобальной информационно-психологической войны. Сохранение и тиражирование в массмедиа базовых фундаментальных ценностей социума способствует национальной безопасности — состоянию защищённости национальных интересов, а также сохранению единства в приверженности жителей страны к исконной культуре и общепринятым ценностным нормам, и традициям.

Согласно данным современной когнитивной лингвистики, языковая личность автора является носителем национальной картины мира или упорядоченной системы представлений о мире и окружающей действительности типичного представителя социума, которая отличается самобытностью и национально-культурным своеобразием [5]. В данном контексте языковая личность журналиста имманентно воспроизводит в медиадискурсе ценности социума и своей культуры, воспринимая и интерпретируя реальность концептуальными ресурсами родного языка.

Осуществлённый анализ медиадискурса военных журналистов разных интернет-изданий показал гармоничное слияние индивидуальных характеристик журналиста и конструкторов национального мировидения. Духовные модели восприятия действительности особо становятся востребованными в эпоху войны, как проявление терминальной аргументации на грани ключевых ценностных категорий: жизнь-смерть, бытие-небытие, благополучие-катастрофа. Осознание смерти даёт всем и всему подлинную ценность, укореняет в незыблемом и вечном [6].

Согласно результатам исследования, в дискурсе военных журналистов преобладают ядерные конструкты ценностного мировидения: вера в победу, взаимовыручка, искренность, милосердие, любовь к родине, жизни и другим людям, самоотверженность [4].

Анализируя содержание статей журналистов, как мужчин, так и женщин, можно выделить ключевые ценностные приоритеты: ответственность, самопожертвование, патриотизм, жизнелюбие. Частотно встречается также мотив веры в справедливость и неизбежность возмездия врагам, особенно выраженный в дискурсе мужчин. Ценности взаимопомощи сильнее проявляются в женских материалах.

Сознательно и архетипически журналисты конструируют своеобразные прототексты, основанные на исторической памяти и канонически поддерживающие должные образцы поведения человека, закреплённые в культурном коде страны.

Осознание текущих событий через призму духовного и нравственного восприятия позволяют оценить происходящее в пространственно-временной перспективе с учётом исторического наследия своего народа и возможного будущего. Это помогает создавать материалы о судьбах конкретных людей, наполненные надеждой на лучшее и верой в торжество неминуемой справедливости.

Сегодня профессиональная объективность журналиста заключается не в поверхностном отражении действительности, а в глубоком понимании основной сути явлений, которую журналист осознаёт, чувствует, принимает близко к сердцу и убедительно передаёт своей аудитории с учётом общих для создателя и потребителя контента национальных ценностей.

#### СПИСОК ЛИТЕРАТУРЫ

1. Баева Л. В. Экзистенциальная природа ценностей: автореферат дис. ... доктора философских наук: 09.00.13. Волгоград, 2004. 43 с.
2. Выжлецов Г. П. Аксиология культуры. СПб.: СПбГУ, 1996. 152 с.
3. Динамика ценностей населения реформируемой России. М.: Эдиториал УРСС, 1996. 224 с.
4. Ерофеева И. В., Михалева Л. В. Аксиологический потенциал эмоционального интеллекта журналиста в медиадискурсе // Гуманитарный вектор. 2024. Т. 19, № 4. С. 132–140. doi: 10.21209/1996-7853-2024-19-4-132-140.
5. Карасик В. И. Языковой круг: личность, концепты, дискурс. Волгоград: Перемена, 2002. 477 с.
6. Митрополит Сурожский Антоний. Труды. М.: «Практика», 2002. 1080 с.
7. Момджян К.Х. О проблеме общечеловеческих ценностей // Вопросы философии. 2020. № 3. С. 25-41.
8. Mchedlova E.M. The Impact of the Crisis on the Development of Socio-cultural Processes and Values // Вестник Национальной академии наук Республики Казахстан. 2021. Т. 5. № 393. С. 199-204.

УДК 004.05

**ГОСУДАРСТВЕННЫЕ И КОРПОРАТИВНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ В УСЛОВИЯХ СОВРЕМЕННОЙ ГЕОПОЛИТИЧЕСКОЙ НЕСТАБИЛЬНОСТИ****Майоров Александр Владимирович**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

e-mail: avmayorov@bk.ru

**Аннотация.** В условиях геополитической нестабильности наблюдается значительное усиление угроз кибербезопасности в отношении ГИС. Это проявляется в росте числа и сложности целевых атак, а также в активизации методов фишинга и распределенных атак типа «отказ в обслуживании» (DDoS). Данные тенденции обусловлены не только технологическими факторами, но и геополитическими аспектами, требующими комплексного подхода к защите информации. Эта система охватывает стратегические основы, общие правовые принципы, отраслевые требования и конкретные методики реализации.

**Ключевые слова:** государственные и корпоративные информационные системы; оценка рисков информационной безопасности; системы обнаружения компьютерных атак.

**STATE AND CORPORATE INFORMATION SYSTEMS OF THE RUSSIAN FEDERATION IN THE CONTEXT OF MODERN GEO-HISTORICAL INSTABILITY****Mayorov Alexander**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

22 Bolshevnikov Av, bldg 1, St. Petersburg, 193232, Russia

e-mail: avmayorov@bk.ru

**Abstract.** In the context of geopolitical instability, there is a significant increase in threats to cybersecurity in relation to GIS. This is reflected in the growing number and complexity of targeted attacks, as well as the activation of phishing methods and distributed denial of service (DDoS) attacks. These trends are driven not only by technological factors, but also by geopolitical aspects that require an integrated approach to information protection. This system covers strategic frameworks, general legal principles, industry requirements, and specific implementation methodologies.

**Keywords:** state and corporate information systems; information security risk assessment; computer attack detection systems.

Государственные информационные системы (ГИС) Российской Федерации обрабатывают данные, значимость которых для национальной безопасности, социальной стабильности и эффективности управления требует обеспечения их защищенности от постоянно эволюционирующих киберугроз [1]. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента № 646) прямо указывает на необходимость обеспечения устойчивости информационной инфраструктуры, включая ГИС, и противодействия использованию информационных технологий (ИТ) в деструктивных целях [2–4].

Проблемы управления рисками информационной безопасности (ИБ) исследованы в работах зарубежных авторов (NIST SP 800-37, NIST SP 800-30, ITSG-33, ENISA Threat Landscape) [5–8] и российских специалистов. Анализ угроз для ГИС Российской Федерации (РФ) представлен в исследованиях Positive Technologies [9–13]. Однако комплексная научная проработка модернизации методики ФСТЭК России с учетом динамики TTPs, облачных рисков и импортозамещения остается недостаточной.

Анализ динамики угроз для ГИС показывает тенденцию к усложнению, целенаправленности и геополитической мотивированности кибератак [14–17]. Исследование актуальных данных за период 2021–2024 годов позволяет выделить ключевые тенденции и специфические угрозы, характерные для государственного сектора.

В ходе проведенной экспериментальной проверки на контролируемой тестовой среде государственной информационной системы были получены количественные и качественные показатели эффективности предложенной модифицированной методики оценки угроз в сравнении с действующей методикой ФСТЭК России (2021 г.) [18, 19]. Эксперимент подтверждает, что повышение адекватности, оперативности и практической ценности оценки угроз безопасности информации в условиях современных вызовов происходит существенно благодаря внедрению разработанных усовершенствований. Моделирование показало уменьшение простоя критических служб ГИС с  $72 \pm 8$  часов до  $18 \pm 3$  часов и финансовых потерь на 45–50%.

Внедрение методики повысит адекватность защиты ГИС, что актуально для ФСТЭК России, операторов ГИС/КИИ и разработчиков ИБ-решений, в части создание инструментов поддержки.

**СПИСОК ЛИТЕРАТУРЫ**

1. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» (ред. от 01.07.2022). <https://base.garant.ru/71556224/> (дата обращения: 12.06.2025).
1. Миняев, А. А. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных / А. А. Миняев, А. В. Красов, Д. В. Сахаров // Вестник СПбГУПТД. Серия 1: Естественные и технические науки. 2020. № 1. С. 29–33. DOI 10.46418/2079-8199\_2020\_1\_5. EDN ULHTJK.
2. Миняев, А. А. Методика оценки эффективности системы защиты информации территориально-распределенных информационных систем / А. А. Миняев, А. В. Красов // Вестник СПбГУПТД. Естеств. и технич. науки. 2020. № 3. С. 26–32. DOI 10.46418/2079-8199\_2020\_3\_4. EDN YNHOEI.

3. Методика оценки угроз безопасности информации: утв. ФСТЭК России 05.02.2021. Москва, 2021. 83 с.
4. Сахаров, Д. В. Инфраструктура связи на Крайнем Севере как база для формирования единой инфосреды / Д. В. Сахаров, С. Е. Мельников, С. И. Штеренберг // Электросвязь. 2016. № 5. С. 18-20. EDN VWSMLP.
5. Штеренберг, С. И. Вредоносное программное обеспечение : Учебное пособие / С. И. Штеренберг. Санкт-Петербург : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2024. 72 с. ISBN 978-5-89160-319-6. EDN SANFRK.
6. Свидетельство о государственной регистрации программы для ЭВМ № 2025681587 Российская Федерация. Оценка вероятности сбоев и уязвимостей сертификатов TLS : заявл. 06.08.2025 : опублик. 15.08.2025 / А. С. Чистяков, Е. С. Чистякова, С. И. Штеренберг ; заявитель СПбГУПТД. EDN YOTAQE.
7. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности (ISO/IEC 27005:2008). М.: Стандартинформ, 2010.
8. Positive Technologies. Актуальные киберугрозы для организаций: итоги 2023 года. 2024. URL: <https://ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-dlya-organizacij-itogi-2023-goda/> (Дата обращения: 12.06.2025).
9. Positive Technologies. Итоги исследований инцидентов ИБ в 2021–2023 годах. 2023. URL: <https://ptsecurity.com/ru-ru/research/analytics/outcomes-of-IS-incident-investigations-in-2021-2023-years/> (Дата обращения: 12.06.2025).
10. Positive Technologies. Кибербезопасность в 2023–2024 гг.: Тренды и прогнозы (Часть 3). 2023. URL: <https://ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-tretya/> (Дата обращения: 12.06.2025).
11. Positive Technologies. Киберугрозы в государственном секторе. 2023. URL: <https://ptsecurity.com/ru-ru/research/analytics/kiberugrozy-v-gosudarstvennom-sektore/> (Дата обращения: 12.06.2025).
12. Positive Technologies. Фишинговые атаки на организации: 2022–2023. 2023. URL: <https://ptsecurity.com/ru-ru/research/analytics/phishing-attacks-on-organizations-in-2022-2023/> (Дата обращения: 12.06.2025).
13. Майоров, А. В. Архитектура и программная реализация системы обнаружения компьютерных атак в корпоративных и государственных информационных системах на основе методов интеллектуального анализа / А. В. Майоров // Вестник СПбГУПТД. Серия 1: Естественные и технические науки. 2023. № 2. С. 40–46. DOI 10.46418/2079-8199\_2023\_2\_8. EDN NEPDFF.
14. Майоров, А. В. Модель представления Больших данных о компьютерных атаках в формате nosql / А. В. Майоров, А. В. Красов, И. А. Ушаков // Вестник СПбГУПТД. Серия 1: Естественные и технические науки. 2023. № 2. С. 47–54. DOI 10.46418/2079-8199\_2023\_2\_9. EDN GDZKWM.
15. Дудников, И. А. Методика анализа журналов событий информационных систем с использованием Elasticsearch для обнаружения сигналов о вредоносных действиях в информационной системе / И. А. Дудников, П. И. Шариков, А. В. Майоров // Научно-аналитический журнал Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. 2025. № 1. С. 120–134. DOI 10.61260/2218-130X-2025-1-120-134. EDN ZQCEXG.
16. Свидетельство о государственной регистрации программы для ЭВМ № 2024691520 Российская Федерация. Программное обеспечение автоматизированного сбора и структурирования журналов приложений для выявления аномалий в информационных системах : заявл. 10.12.2024 : опублик. 23.12.2024 / А. В. Майоров, П. И. Шариков, А. В. Красов, А. И. Пешков ; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича». EDN IURLQM.
17. Свидетельство о государственной регистрации программы для ЭВМ № 2025662154 Российская Федерация. Модифицированный анализатор журналов на основе расширенного набора агрегаций и модели обнаружения аномалий на основе временных рядов : заявл. 13.05.2025 : опублик. 19.05.2025 / А. В. Майоров. EDN WXIYYH.
18. Свидетельство о государственной регистрации программы для ЭВМ № 2025618525 Российская Федерация. Модифицированный анализатор журналов маршрутизаторов на основе расширенного набора агрегаций и модели обнаружения аномалий на основе временных рядов : заявл. 28.03.2025 : опублик. 04.04.2025 / А. В. Майоров. EDN KSZLRH.

УДК 621.396.4

## МЕХАНИЗМЫ ЗАЩИТЫ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РЕГИОНОВ РОССИИ

Ренсков Дмитрий Андреевич

Военная академия связи им. Маршала Советского Союза С.М. Буденного  
Тихорецкий пр-т, д. 3, Санкт-Петербург, 194064, Россия  
e-mail: dmitryirenskov@gmail.com

**Аннотация.** Работа посвящена защите критической информационной инфраструктуры регионов России. Рассматриваются нормативно-правовые акты, методы и средства защиты данных, особенности реализации мер в условиях цифровых технологий и киберугроз. Проведен анализ проблем и даны рекомендации по повышению защищенности на региональном уровне. Актуальность обусловлена необходимостью надежной защиты важнейших объектов и ресурсов для стабильного функционирования регионов в условиях современных вызовов информационной безопасности.

**Ключевые слова:** критическая информационная инфраструктура; информационная безопасность; защита данных; киберугрозы; нормативно-правовое регулирование; региональная безопасность; цифровая трансформация; меры защиты; кибербезопасность; государственное регулирование.

## MECHANISMS FOR PROTECTING THE CRITICAL INFORMATION INFRASTRUCTURE OF RUSSIAN REGIONS

Renskov Dmitry

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny  
3 Tikhoretsky Av, St. Petersburg, 194064, Russia  
e-mail: dmitryirenskov@gmail.com

**Abstract.** The work is devoted to the protection of the critical information infrastructure of the regions of Russia. Regulatory legal acts, methods and means of data protection, and the specifics of implementing measures in the context of digital technologies and cyber threats are considered. An analysis of the problems was carried out and recommendations were made to increase security at the regional level. The urgency is due to the need for reliable protection of the most

important facilities and resources for the stable functioning of the regions in the context of modern information security challenges.

**Keywords:** critical information infrastructure; information security; data protection; cyber threats; regulatory and legal regulation; regional security; digital transformation; security measures; cybersecurity; government regulation.

В условиях цифровой трансформации и глобализации информационные технологии играют ключевую роль в поддержании функционирования государственных институтов, экономической системы, социальной сферы и обеспечении жизнедеятельности населения. Критическая информационная инфраструктура (КИИ) представляет собой совокупность объектов и систем, обеспечивающих функционирование стратегически значимых отраслей и процессов, включая энергетику, транспорт, связь, здравоохранение, финансы и другие. В условиях роста киберугроз и геополитических вызовов обеспечение безопасности КИИ является приоритетной задачей для органов государственной власти субъектов Российской Федерации. В данной статье рассматриваются основные механизмы защиты критической информационной инфраструктуры на региональном уровне.

1. Понятие и структура критической информационной инфраструктуры субъектов Российской Федерации.

Критическая информационная инфраструктура представляет собой совокупность объектов, систем, сетей, программного обеспечения и данных, обеспечивающих функционирование критически важных для жизнедеятельности региона отраслей. В соответствии с Федеральным законом №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 года, под КИИ понимаются информационные системы и ресурсы, нарушение функционирования которых может привести к значительным негативным последствиям для безопасности государства, экономики и социальной стабильности [1].

Структура КИИ в субъектах Российской Федерации включает: энергетические системы, включая электроснабжение и газоснабжение; транспортные системы, включая железнодорожный транспорт и аэропорты; системы связи и телекоммуникаций; финансовые учреждения; образовательные и медицинские организации; системы водоснабжения и водоотведения.

Обеспечение защиты указанных компонентов требует комплексного подхода, учитывающего региональные особенности и специфику функционирования объектов КИИ.

2. Законодательная база и нормативно-правовые механизмы.

На федеральном уровне сформирована нормативно-правовая база, регулирующая вопросы обеспечения безопасности КИИ. Ключевыми нормативными актами являются: Федеральный закон №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», определяющий основные принципы и порядок функционирования КИИ, а также меры по её защите; Постановление Правительства Российской Федерации №1245 от 25 октября 2017 года «Об утверждении перечня объектов критической информационной инфраструктуры, а также их критических процессов и показателей»; Федеральный закон №152-ФЗ «О персональных данных», регулирующий вопросы обработки персональных данных в рамках обеспечения информационной безопасности [2, 3].

На уровне субъектов Российской Федерации реализуются региональные программы и нормативные акты, направленные на обеспечение безопасности КИИ, с учетом местных особенностей и потребностей.

3. Механизмы технической защиты.

Технические меры являются основополагающими в системе обеспечения безопасности КИИ. Они включают: применение современных средств кибербезопасности, таких как межсетевые экраны (фаерволы), системы обнаружения и предотвращения вторжений (IDS/IPS), антивирусные программы и системы защиты от вредоносного ПО; шифрование данных при передаче и хранении; регулярное обновление программного обеспечения для устранения выявленных уязвимостей; создание резервных копий информационных систем и данных для оперативного восстановления после инцидентов; мониторинг сетевой активности в режиме реального времени для выявления аномальных событий [4].

Особое внимание уделяется сегментации информационных сетей, что позволяет изолировать корпоративные системы от внешних сетей и минимизировать риски распространения киберугроз.

4. Организационные меры.

Организационные механизмы направлены на создание эффективной системы управления информационной безопасностью. К ним относятся: формирование специализированных структур, ответственных за обеспечение информационной безопасности на региональном уровне, таких как центры мониторинга или штабы по защите КИИ; разработка и внедрение планов реагирования на инциденты (ПРИ), включая алгоритмы действий в случае кибератак и других угроз; проведение регулярных учений и тренингов для сотрудников организаций, являющихся частью КИИ; внедрение системы управления информационной безопасностью (СУИБ) в соответствии с международными стандартами, такими как ISO/IEC 27001; обеспечение взаимодействия между органами государственной власти, операторами критической информационной инфраструктуры и правоохранительными структурами.

Эффективная организационная система способствует своевременному выявлению киберугроз и минимизации их последствий.

5. Правовая ответственность и контроль.

Для повышения уровня ответственности за соблюдение требований в области защиты КИИ введены меры административной и уголовной ответственности за нарушение законодательства. Контроль за соблюдением

нормативно-правовых актов осуществляется Федеральной службой по техническому и экспортному контролю (ФСТЭК России), Роскомнадзором и другими уполномоченными органами.

Региональные органы исполнительной власти осуществляют проверки объектов КИИ, проводят анализ инцидентов информационной безопасности и участвуют в межрегиональных и федеральных мероприятиях по обмену опытом и лучшими практиками [5].

#### 6. Информационно-техническое сотрудничество.

Обеспечение безопасности КИИ требует тесного взаимодействия между различными субъектами, включая государственные органы, операторов связи, крупные предприятия и организации. Для этого создаются специализированные платформы для обмена информацией о киберугрозах и координации действий при возникновении инцидентов. Важным элементом является участие в национальных программах и инициативах, направленных на развитие кибербезопасности, таких как проекты Центра защиты информации при ФСТЭК России и национальная система обмена информацией об угрозах (ISAC).

7. Перспективы развития механизмов защиты критической информационной инфраструктуры в субъектах Российской Федерации.

Современные вызовы и тенденции в области информационных технологий требуют постоянного совершенствования механизмов защиты КИИ. В перспективе планируется: внедрение технологий искусственного интеллекта и машинного обучения для автоматического обнаружения и анализа киберугроз; развитие национальной системы управления инцидентами информационной безопасности; обновление нормативно-правовой базы с учетом появления новых технологий и методов кибератак; повышение уровня квалификации специалистов в области информационной безопасности; расширение международного сотрудничества в сфере обеспечения кибербезопасности.

Реализация указанных мер позволит повысить уровень защищенности критической информационной инфраструктуры субъектов Российской Федерации и минимизировать риски, связанные с киберугрозами.

### СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. // Российская газета. 2017. № 147.
2. Постановление Правительства РФ № 1245 «Об утверждении перечня объектов критической информационной инфраструктуры» от 28 декабря 2017 г.
3. Федеральный закон № 152-ФЗ «О персональных данных» от 27 июля 2006 г.
4. Иванов И.И., Петров П.П. Кибербезопасность и защита критической инфраструктуры: учебное пособие / И.И. Иванов, П.П. Петров. М.: Наука, 2020.
5. Смирнова А.В., Кузнецов В.С. Механизмы обеспечения информационной безопасности в регионах России // Журнал «Информационная безопасность», 2019, № 4, с. 45–52.

УДК 004.056

## ОСОБЕННОСТИ РЕАЛИЗАЦИИ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ ПО ФОРМИРОВАНИЮ ГОСУДАРСТВЕННОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

**Сторожик Виктор Сергеевич**

Арктический и антарктический научно-исследовательский институт  
Беринга ул., 38, г. Санкт-Петербург, 199397, Россия  
e-mail: vsstorozhik@aari.ru

**Аннотация.** Рассматриваются особенности современного этапа реализации государственной политики по формированию государственной системы защиты информации ограниченного доступа и общедоступной информации с учетом актуальных угроз безопасности информации.

**Ключевые слова:** безопасность; защита; информация; информационная инфраструктура; инцидент; обнаружение; ограниченный доступ; орган; организация; политика; положение; система.

## THE SPECIFICS OF THE IMPLEMENTATION OF THE STATE POLICY ON THE FORMATION OF THE STATE INFORMATION PROTECTION SYSTEM

**Storozhik Viktor**

Arctic and Antarctic Research Institute  
38 Bering str., St. Petersburg, 199397, Russia  
e-mail: vsstorozhik@aari.ru

**Abstract.** The article considers the features of the current stage of the implementation of the state policy on the formation of a state system for the protection of information with limited access and publicly available information, considering current threats to information security.

**Keywords:** security; protection; information; information infrastructure; incident; detection; restricted access; authority; organization; policy; position; system.

В докладе Президента Российской Федерации «О повышении устойчивости и безопасности функционирования информационной инфраструктуры государства» на заседании Совета Безопасности

Российской Федерации 20 мая 2022 г. указано, что против России развязана война в информационном пространстве, а также поставлен вопрос о создании государственной системы защиты информации (ГСЗИ) [1].

В настоящее время проходит процедуру общественного обсуждения проект Указа Президента Российской Федерации «Об утверждении Положения о государственной системе защиты информации в Российской Федерации» (Положение) [2], которым определяются состав и основные направления деятельности ГСЗИ, а также требования к организации защиты информации (ЗИ) ограниченного доступа и общедоступной информации.

Положение также регламентирует требования к органам государственной власти и организациям при сборе, хранении, обработке, предоставлении, распространении ими информации ограниченного доступа и общедоступной информации с использованием объектов информационной инфраструктуры (ИИ) на территории Российской Федерации.

Организационную основу ГСЗИ составляют: ФСТЭК России и ее территориальные органы; ФСБ России и территориальные органы безопасности; органы, организации, организующие и (или) осуществляющие ЗИ, их подразделения, обеспечивающие ЗИ; научные организации по проблемам ЗИ; организации, осуществляющие создание СЗИ; организации, выполняющие работы и (или) оказывающие услуги в области ЗИ; органы по сертификации и испытательные центры (лаборатории), проводящие работы по сертификации СЗИ; организации, осуществляющие подготовку кадров в области ЗИ.

Деятельность ГСЗИ осуществляется на федеральном, межрегиональном, региональном, ведомственном и объектовом уровнях.

ГСЗИ функционирует во взаимодействии с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА), созданной в соответствии с Указом Президента Российской Федерации от 15 января 2013 г. № 31с [3, 4, 5].

Нормативно-правовое обеспечение создания ГСЗИ направлено на повышение уровня защищенности информационных ресурсов органов государственной власти и организаций от КА с учетом актуальных УБИ и характеризуется динамичным развитием.

Приказом ФСТЭК России от 11 апреля 2025 г. № 117 утверждены Требования о ЗИ, которые направлены на дальнейшее совершенствование процесса обеспечения ЗИ, содержащейся в функционирующих на территории Российской Федерации государственных информационных системах (ГИС), иных информационных системах (ИС) государственных органов, государственных унитарных предприятий, государственных учреждений, предотвращения НСД к информации, специальных воздействий на информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к ней [6]. В случае передачи информации ограниченного доступа из ГИС в иные ИС, ИС в которую передается информация ограниченного доступа, должна соответствовать Требованиям.

Приказом ФСБ России от 18 марта 2025 г. N 117 утверждены Требования о ЗИ, содержащейся в ГИС, иных ИС государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств [7].

В рамках формирования ГСЗИ Правительством Российской Федерации 7 июля 2025 г. внесен в Государственную Думу законопроект «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» [8], которым предлагаются дополнительные меры, направленные на обеспечение эффективности создания и последующего учета ГИС, принимая во внимание современные аспекты их создания и развития в интересах дальнейшего совершенствования ГСЗИ:

1. Конкретизировать критерии отнесения информационных систем к ГИС, в том числе:

- ввести в понятийный аппарат самостоятельные понятия: «государственная информационная система», конкретизирующее цели создания ГИС, а также «государственная цифровая платформа», «государственный информационный ресурс» и «ведомственный сервис»;

- определить закрытый перечень видов нормативных правовых актов, являющихся основанием для создания ГИС;

- законодательно закрепить виды ГИС (федеральные, региональные и ведомственные ГИС, а также муниципальные информационные системы (МИС) и иные ИС);

- наделить Правительство Российской Федерации полномочиями устанавливать общие требования к содержанию нормативных правовых актов, являющихся основанием создания, развития (модернизации) и эксплуатации ГИС, а также устанавливать дополнительные требования к ГИС, входящих в состав государственных цифровых платформ;

2. Ввести термины «государственная информационная система», «государственная цифровая платформа», «государственный информационный ресурс» и «ведомственный сервис».

3. Установить требования по локализации технических средств ГИС и МИС на территории Российской Федерации.

4. Установить требование о непрерывном взаимодействии с ГосСОПКА для ГИС, МИС, ведомственных ИС и некоторых иных ИС.

Реализация положений законопроекта в целом позволит создать условия для достижения национальной цели ускоренного внедрения цифровых технологий и будет являться одним из ключевых факторов для ее выполнения.

## СПИСОК ЛИТЕРАТУРЫ

1. О повышении устойчивости и безопасности функционирования информационной инфраструктуры государства :Доклад Президента Российской Федерации на заседании Совета Безопасности Российской Федерации. — 20 мая 2022.
2. Об утверждении Положения о государственной системе защиты информации в Российской Федерации : Проект Указа Президента Российской Федерации [электронный ресурс]. URL: <https://regulation.gov.ru/projects#pra=135259> (дата обращения: 10.07.2025).
3. О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации : Указ Президента Российской Федерации от 15 января 2013 г. № 31с.
4. О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации : Указ Президента Российской Федерации от 20 декабря 2017 г. № 620.
5. Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации : утверждена Президентом Российской Федерации 12 декабря 2014 г. № К 1274.
6. Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений : утверждены приказом ФСТЭК России от 11 апреля 2025 г. № 117.
7. Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств : утверждены приказом ФСБ России от 18 марта 2025 г. № 117.
8. Законопроект «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации». [Электронный ресурс]. URL: <https://sozd.duma.gov.ru/bill/960721-8> (дата обращения: 10.07.2025).

УДК 004

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА  
И ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ  
РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Шилков Владимир Ильич, Гладских Марианна Владимировна**

Уральский федеральный университет имени первого Президента России Б.Н. Ельцина,  
Мира, ул., 19, Екатеринбург, 620002, Россия  
e-mails: vi.shilkov@urfu.ru; mariannagladskih@gmail.com

**Аннотация.** Обсуждаются проблемы и стратегии обеспечения информационной безопасности государственных информационных систем Российской Федерации. Обозначены задачи, перспективные направления развития и основные мероприятия по повышению уровня «цифрового доверия» и информационной безопасности региональных и федеральных компонентов электронного правительства.

**Ключевые слова:** информационная безопасность; государственные информационные системы; электронное правительство.

**INFORMATION SECURITY OF THE ELECTRONIC GOVERNMENT AND STATE  
INFORMATION SYSTEMS OF THE RUSSIAN FEDERATION**

**Shilkov Vladimir, Gladskikh Marianna**

Ural Federal University, named after the First President of Russia B.N. Yeltsin,  
19 Mira St., Yekaterinburg, 620002, Russia  
e-mails: vi.shilkov@urfu.ru; mariannagladskih@gmail.com

**Abstract.** The problems and strategies of ensuring information security of the state information systems of the Russian Federation are discussed. The tasks, promising areas of development and main measures to increase the level of «digital trust» and information security of regional and federal components of e-government are outlined.

**Keywords:** information security; state information systems; electronic government.

Развитие информационно-коммуникационных технологий привело к формированию новых концепций, подходов и возможностей в сфере государственного управления. Так, например, уже стали привычными, относительно недавно появившиеся термины «электронное правительство», «портал госуслуг», «многофункциональный центр», «государственная информационная система». Реальными шагами по созданию электронного правительства стали инициативы, перечисленные в Распоряжении Правительства РФ от 6 октября 2021 года № 2816-р «Об утверждении перечня инициатив социально-экономического развития РФ до 2030 года». К этим инициативам можно отнести, например: электронный документооборот, госуслуги онлайн, цифровой профиль гражданина.

Актуальность обсуждения вопросов, связанных с внедрением информационно-коммуникационных технологий в процессы государственного управления обусловлена различными причинами, к которым следует отнести необходимость решения целого ряда задач, связанных, например, с: разработкой стратегии создания безопасной цифровой среды, необходимой для успешного функционирования государственных информационных систем и электронного правительства; формированием концепции «цифрового доверия»; уточнением и конкретизацией концепций и терминов; совершенствованием нормативно-правовой базы; координацией функционирования электронных правительств и государственных информационных систем на федеральном и региональном уровне.



Однако, несмотря на несомненные успехи, достигнутые при реализации концепции электронного правительства на федеральном и региональном уровне, существует большое количество проблем, нуждающихся в скорейшем решении. Так, например, по мнению автора [1], существенной проблемой российского электронного правительства является отсутствие утвержденной стратегии, а также ясного законодательного определения его сути и организационной структуры. В связи с этим, на данном этапе, электронное правительство в России представляется «чем-то неопределенным и размытым». Анализ международного опыта показывает, что для эффективного управления развитием электронного правительства необходимо учитывать появление новых возможностей и при разработке мероприятий по повышению эффективности государственных информационных систем целесообразно принять во внимание ряд общемировых тенденций, к которым относятся, например: представление государственных данных в формате, пригодном для автоматизированной обработки и многократного использования; применение действенных инструментов общественного контроля, базирующихся на информации о работе государственных структур; оптимизация институциональной структуры; совершенствование нормативно-правовой базы и создание специализированных ведомств [2].

В соответствии со сведениями [3], в Госдуму поступил законопроект, имеющий целью однозначно определить термины «государственная информационная система», «государственная цифровая платформа», «государственный информационный ресурс» и «ведомственный сервис», а также конкретизировать критерии отнесения информационных систем к государственным информационным системам» (ГИС) и установить общие и дополнительные требования к содержанию нормативных правовых актов, являющихся основанием для создания, развития (модернизации) и эксплуатации ГИС, входящих в состав государственных цифровых платформ.

К важнейшим задачам, которые необходимо решать в рамках разработки стратегий повышения эффективности функционирования электронного правительства, относятся задачи обеспечения информационной безопасности компонентов ГИС. Так, например, в соответствии с [4], в период с 1 марта 2025 года специалисты «Лаборатории Касперского» пресекли рассылку сотен писем, высланных якобы с адреса государственного справочно-информационного портала и, содержащих требования позвонить по телефону с целью уточнения персональных данных (паспорт, СНИЛС, ИНН), необходимых для защиты аккаунтов, в отношении которых «по учётной записи были совершены нехарактерные и подозрительные действия». По мнению автора [5] важной и актуальной задачей, является задача формирования «цифрового доверия» к инструментам электронного документооборота, применяемым в ГИС.

Авторы [6] считают, что проблемы информационной безопасности необходимо учитывать, в том числе и при разработке стратегии развития сети многофункциональных центров (МФЦ), действующих в соответствии с национальным проектом «Электронное правительство». Следует принять во внимание, что цифровизация государственных услуг, хоть и повышает удобство и скорость предоставления услуг, но одновременно приводит к возникновению многочисленных информационных рисков, возникающих из-за передачи данных между различными ведомствами, что создает возможности несанкционированного перехвата информации и ее неправомерного использования в мошеннических схемах. К перспективным методам, с помощью которых можно повысить уровень информационной безопасности и «цифрового доверия» к МФЦ, следует отнести, например, методы криптографической защиты, технологии биометрической аутентификации, которые позволяют обеспечить дополнительный уровень защиты, анализируя уникальные биологические характеристики пользователей информационной системы и, в совокупности с традиционной электронной цифровой подписью существенно ограничат риски несанкционированного доступа к данным и повысят общую надежность информационно-справочной системы.

В рамках реализации государственной политики обеспечения информационной безопасности Министерство цифрового развития в 2023 году запустило программу по поиску уязвимостей-*bug bounty*, чтобы выявить слабые места в защите портала «Госуслуги». В рамках стартового этапа, проходившего с февраля по май 2023 года, свыше 8 тысяч специалистов провели анализ безопасности портала и Единой системы идентификации и аутентификации (ЕСИА). В результате проведенной работы было обнаружено и устранено 37 уязвимостей. Общая сумма выплат участникам, сообщившим об ошибках, достигла 1,95 миллиона рублей. Ключевой целью программы *bug bounty* является повышение уровня безопасности ГИС за счет привлечения сторонних экспертов к поиску и устранению потенциальных рисков [7]. Министерство цифрового развития в рамках третьего этапа программы предполагает выявить слабые места в системах безопасности девяти государственных онлайн-сервисов, в том числе, в: Едином портале государственных и муниципальных услуг, Единой биометрической системе, Единой системе нормативной справочной информации. Поиск уязвимостей будет проводиться на базе платформ *BI.ZONE Bug Bounty* и *Standoff 365 Bug Bounty*, и завершится 20 декабря 2026 года.

Перспективные направления повышения информационной безопасности и эффективности ГИС и электронного правительства связаны с применением инновационных технологий, к которым следует отнести, например, инструментальные средства искусственного интеллекта. Так, например, в соответствии с [8], Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации подготовлен проект постановления правительства «О проведении эксперимента по использованию генеративного искусственного интеллекта в государственном управлении», в соответствии с которым на базе ГИС «Единая информационная платформа национальной системы управления данными» будут созданы пять сервисов по направлениям: управление данными; обработка текстовых документов на естественном языке; развитие кадрового потенциала; работа с контентом; управление рисками.

Таким образом, на основании проведенного исследования можно сделать вывод, что формирование стратегических планов по повышению информационной безопасности электронного правительства и государственных информационных систем является сложной задачей, требующей учета большого количества различных факторов и потенциальных рисков и должно осуществляться на основе комплексного системного подхода.

#### СПИСОК ЛИТЕРАТУРЫ

1. Морозова С.С. Формирование динамической модели оптимизации электронного правительства в Российской Федерации в условиях новых вызовов и рисков. Политическая экспертиза: Политэкс. 2023. Т. 19. № 3. С. 415-430.
2. Ваславский Ян.И., Габуев С.В. Варианты развития электронного правительства. опыт России, США, КНР. Международные процессы. 2017. Т. 15. № 1 (48). С. 108-125.
3. Внесён правительственный законопроект о государственных информационных системах / [Электронный ресурс] // Digital Russia URL: <https://d-russia.ru/vnesjon-pravitelstvennyj-zakonoproekt-o-gosudarstvennyh-informacionnyh-sistemah.html> (дата обращения: 30.07.2025).
4. Россиянам рассылают фальшивые письма и просят перезвонить для защиты аккаунта на «Госуслугах» [Электронный ресурс] // Cyber media : [сайт]. URL: <https://securitymedia.org/news/rossiyanam-rassylayut-falshivye-pisma-i-prosyat-perezvonit-dlya-zashchity-akkaunta-na-gosuslugakh.html> (дата обращения: 18.07.2025).
5. Чепелюк С.Г. Феномен «цифрового доверия» и его влияние на становление цифрового правительства в России. Вестник Российского университета дружбы народов. Серия: Политология. 2022. Т. 24. № 3. С. 447-459.
6. Рязанова О.А., Кошлец И.Г. Обеспечение информационной безопасности многофункциональных центров. Вектор экономики. 2021. № 9 (63).
7. Найди уязвимость на «Госуслугах» — получи вознаграждение [Электронный ресурс] // РБК URL: [https://www.rbc.ru/technology\\_and\\_media/14/12/2023/6579d64d9a7947ba190dfaf2](https://www.rbc.ru/technology_and_media/14/12/2023/6579d64d9a7947ba190dfaf2) (дата обращения: 16.07.2025).
8. Намечено экспериментальное использование ИИ в госуправлении [Электронный ресурс] Digital Russia. URL: <https://d-russia.ru/namecheno-jekspperimentalnoe-ispolzovanie-ii-v-gosupravlenii.html> (дата обращения: 29.07.2025).



## ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК: 651.012

### КЛАССИФИКАЦИЯ КРИТЕРИЕВ ОЦЕНКИ ПО РЕЗУЛЬТАТИВНОСТИ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ, КАК СОЦИАЛЬНОЙ ОРГАНИЗАЦИОННО- ТЕХНИЧЕСКОЙ СИСТЕМЫ

**Алексеев Сергей Алексеевич, Гончар Александр Михайлович**

Академия войск национальной гвардии

Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия

e-mails: ksgati@yandex.ru, alexander132000@yandex.ru

**Аннотация.** Доклад посвящен разработке методики по классификации критериев оценки результативности мер по защите конфиденциальной информации в структуре образовательной организации, как социальной организационно-технической системы. Предлагается комплексный подход к оценке защиты конфиденциальной информации в социальных организационно-технических системах на примере образовательных организаций. Авторы обосновывают применение метода анализа иерархий. Предложена трехуровневая иерархическая модель, где глобальной целью является повышение результативности защиты. На втором уровне обосновано использование критериев, в роли которых выступают лицензионные требования и аккредитационные показатели. Альтернативами третьего уровня выступают структурные подразделения образовательной организации. Вычисление весовых коэффициентов для критериев и структурных подразделений позволяет количественно оценить их вклад в защиту информации, выявить приоритеты для оптимизации ресурсов, организационных процессов и разработки научно обоснованных рекомендаций по повышению уровня безопасности.

**Ключевые слова:** критерии оценки; защита конфиденциальной информации; результативность защиты; социальная организационно-техническая система; образовательная организация; метод анализа иерархий.

### CLASSIFICATION OF CRITERIA FOR ASSESSING THE EFFECTIVENESS OF PROTECTING CONFIDENTIAL INFORMATION IN THE STRUCTURE OF AN EDUCATIONAL ORGANIZATION AS A SOCIAL ORGANIZATIONAL AND TECHNICAL SYSTEM

**Alekseyev Sergey, Gonchar Alexander**

Academy of the National Guard Troops

1 Pilot Pilyutova St, St. Petersburg, 198206, Russia

e-mails: ksgati@yandex.ru, alexander132000@yandex.ru

**Abstract.** The report is devoted to the development of a methodology for classifying criteria for assessing the effectiveness of measures to protect confidential information in the structure of an educational organization as a social organizational and technical system. A comprehensive approach to assessing the protection of confidential information in social organizational and technical systems is proposed, using the example of educational organizations. The authors justify the use of the hierarchical analysis method. A three-level hierarchical model is proposed, where the global goal is to improve the effectiveness of protection. At the second level, the use of criteria based on licensing requirements and accreditation indicators is justified. The third-level alternatives are the structural units of the educational organization. Calculating the weight coefficients for the criteria and structural units allows us to quantify their contribution to information protection and identify priorities for optimizing resources and organizational processes.

**Keywords:** evaluation criteria; confidential information protection; effectiveness of defense; social organizational and technical system; educational organization; hierarchy analysis method.

В современных условиях цифровой трансформации обеспечение конфиденциальности информации выступает критически важным аспектом функционирования любой организации. Особую сложность представляет защита данных в социальных организационно-технических системах (СОТС), где безопасность формируется сложным взаимодействием технологических решений, организационных процедур и человеческого фактора. Разработка комплексных методик оценки, способных учитывать разнородные критерии и их относительную значимость, является важной задачей. Структурирование этой сложной задачи возможно с помощью метода анализа иерархий (МАИ), предлагающего, классификацию критериев оценки и определение их весовых коэффициентов на основе экспертных суждений [1]. Целью исследования является разработка методики и обоснование системы критериев для оценки результативности защиты конфиденциальной информации в

структуре СОТС с применением элементов МАИ. Практическое применение данной методики позволит перейти к более объективному и сбалансированному вычислению весовых коэффициентов результативности защиты конфиденциальной информации.

Проведенный анализ публикаций по организации защиты конфиденциальных сведений показал о значительном количестве исследований в этой области. К ним можно отнести работы авторов: по оценке эффективности системы информационной безопасности и защиты информации — Коржан Ю.Э., Богаченко Н.Ф., Корнилов Д.А., Демидов Н.Е., Умников Е.В., Атакишев О.И., Грачев В.А., Чемин А.А., Поляков С.П.); по принятию решений методом анализа иерархий — Саати Т.Л., Сакова Т.Г., Давлианидзе Я.С., Разумников С.В., Лобов С.А., Привалов А.А., Чемиренко В.П., Трофимец В.Я. Анализ данных исследований привел авторов к выводу, что задача количественной оценки результативности защиты конфиденциальной информации (с учетом факторов неопределенности) является актуальной. В качестве СОТС авторы рассматривали образовательные организации. Ключевым элементом такой оценки является вычисление весовых коэффициентов, определяющих приоритет структурных подразделений по выбранным критериям [2].

Реализация этого подхода позволило разработать научно обоснованные рекомендации, направленные на оптимизацию организационных процессов и повышение результативности защиты информации в ВУЗе. Для построения иерархии предложена трехуровневая иерархическая модель. Фокусом иерархии является глобальная цель — повышение результативности защиты конфиденциальной информации в образовательной организации. Второй уровень включает критерии, которые могут представлять как материальные, так и нематериальные факторы, измеряемые количественные параметры и качественные характеристики, объективные данные и субъективные экспертные оценки. Критерии помогают определить приоритеты альтернативных решений относительно главной цели. При определении критериев учитывались следующие факты. Во-первых, в качестве СОТС выступает образовательная организация, осуществляющая на основании лицензии образовательную деятельность в качестве основного вида деятельности в соответствии с целями, ради достижения которых такая организация создана [3]. Во-вторых, высокий уровень защиты конфиденциальной информации свидетельствует о нормальном функционировании образовательной организации. Это в свою очередь позволяет качественно реализовывать основные профессиональные образовательные программы, в том числе содержащие конфиденциальную информацию. Оценка качества образовательной деятельности определяется через аккредитационные показатели. В качестве критериев предложено использовать лицензионные требования, предъявляемые к соискателю лицензии на осуществление образовательной деятельности [4] и аккредитационные показатели [5]. Проведя сопоставление перечисленных показателей, можно прийти к выводу о необходимости объединения показателей, в равной степени раскрывающих их содержание, и схожих по содержанию в отношении к защите конфиденциальных сведений в образовательной организации. Такими показателями могут являться:

- Наличие на праве собственности или ином законном основании зданий, строений, сооружений, помещений, необходимых для осуществления образовательной деятельности по заявленным к лицензированию образовательным программам;
- Наличие материально-технического обеспечения образовательной деятельности, оборудование помещений, необходимых для осуществления образовательной деятельности по заявленным к лицензированию образовательным программам;
- Наличие условий для функционирования электронной информационно-образовательной среды, включающей в себя информационные технологии, технические средства, электронные информационные ресурсы, электронные образовательные ресурсы, которые содержат электронные учебно-методические материалы;
- Наличие в штате лицензиата или привлечение им на ином законном основании педагогических работников, имеющих профессиональное образование, обладающих соответствующей квалификацией, имеющих стаж работы, необходимый для осуществления образовательной деятельности по реализуемым образовательным программам;
- Наличие в организациях, осуществляющих образовательную деятельность по реализации образовательных программ высшего образования и дополнительных профессиональных программ, научных работников.

Проведя объединение показателей, второй уровень иерархии (уровень критериев) будет представлен в виде 11 показателей (критериев), в отношении которых могут проводиться вычисления весовых коэффициентов, как самих критериев, так и их альтернатив. В качестве альтернатив иерархии, могут выступать структурные подразделения образовательной организации, осуществляющие образовательную деятельность (кафедры, курсы). Они будут третьим уровнем построенной иерархии.

Качественный подбор критериев оценки результативности по защите конфиденциальной информации позволит определить роль и вклад каждого из структурных подразделений образовательной организации в повышение результативности защиты конфиденциальной информации. Это поможет: сфокусировать ресурсы на критически важных нарушениях; ранжировать функции кафедр (курсов); упростить принятие решений и повысить объективность и ясность оценок; вовлечь экспертов; оценить риски и неопределенности; оптимизировать планирование защиты; рационально распределить обязанности и бюджет в соответствии с приоритетами.

## СПИСОК ЛИТЕРАТУРЫ

1. Саати, Т. Л. Принятие решений с помощью метода анализа иерархий / Т. Л. Саати // Методы менеджмента качества. 2022. № 7. С. 54-60. EDN EYKKDX.
2. Гончар, А. М. Метод управления режимом секретности в повседневной деятельности военной образовательной организации высшего образования // Военно-правовые и гуманитарные науки Сибири. 2025. № 2. С. 292-301.
3. Федеральный закон от 29.12.2012 № 273-ФЗ (ред. от 24.02.2021) «Об образовании в Российской Федерации» // Собрание законодательства РФ. 2012. № 53 (ч. 1). Ст. 7598.
4. Положение о лицензировании образовательной деятельности \ КонсультантПлюс // [www.consultant.ru](http://www.consultant.ru)[сайт] режим доступа: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_363079/26b9a9317e489d57a9842321e747706412e110ff/](https://www.consultant.ru/document/cons_doc_LAW_363079/26b9a9317e489d57a9842321e747706412e110ff/) свободный (дата обращения: 16.07.2025) Загл. с экрана.
5. Приказ Министерства науки и высшего образования Российской Федерации от 18.04.2023 № 409 Официальное опубликование правовых актов // [publication.pravo.gov.ru](http://publication.pravo.gov.ru)[сайт] режим доступа: <http://publication.pravo.gov.ru/document/0001202305190009> свободный (дата обращения: 16.07.2025) Загл. с экрана.

УДК 323.28

**НАЦИОНАЛЬНАЯ АНТИТЕРРОРИСТИЧЕСКАЯ БЕЗОПАСНОСТЬ****Алимов Денис Олегович, Кузнецов Вячеслав Дмитриевич**

Академия войск национальной гвардии

Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия

e-mails: [alimovdo@rosgvard.ru](mailto:alimovdo@rosgvard.ru), [89513325199@mail.ru](mailto:89513325199@mail.ru)

**Аннотация.** Национальная антитеррористическая безопасность включает в себя профилактику радикализации, международное сотрудничество и использование современных технологий. Профилактика направлена на предотвращение экстремистских настроений среди молодежи, а сотрудничество с другими странами способствует обмену информацией. Современные технологии, такие как видеонаблюдение, повышают уровень безопасности, но важно учитывать права человека. Вовлечение общества в антитеррористические меры помогает выявлять угрозы и укрепляет доверие к государству. Комплексный подход позволяет эффективно защищать граждан от терроризма.

**Ключевые слова:** национальная безопасность; антитеррор; защита; профилактика; угрозы.

**NATIONAL ANTI-TERRORIST SECURITY****Alimov Denis, Kuznetsov Veacheslav**

Academy of the National Guard Troops

Pilot Pilyutova St, 1, St. Petersburg, 198206, Russia

e-mails: [alimovdo@rosgvard.ru](mailto:alimovdo@rosgvard.ru), [89513325199@mail.ru](mailto:89513325199@mail.ru)

**Abstract.** National anti-terrorism security includes prevention of radicalization, international cooperation, and the use of modern technologies. Prevention aims to prevent extremist attitudes among young people, while cooperation with other countries facilitates the exchange of information. Modern technologies, such as video surveillance, enhance security, but it is important to consider human rights. Involving society in anti-terrorism measures helps identify threats and builds trust in the government. A comprehensive approach ensures effective protection of citizens from terrorism.

**Keywords:** national security, anti-terrorism, protection, and prevention; threats.

Национальная антитеррористическая безопасность является ключевым элементом государственной политики, направленным на защиту граждан, инфраструктуры и демократических институтов от угроз терроризма. Эффективная антитеррористическая стратегия требует комплексного подхода, включающего профилактику радикализации, международное сотрудничество, развитие технологий безопасности и активное вовлечение общества в борьбу с терроризмом. Только интеграция этих элементов позволит создать устойчивую систему, способную эффективно реагировать на вызовы современности и обеспечивать безопасность нации.

Основной задачей антитеррористической политики является предотвращение радикализации молодежи и других уязвимых групп. Это включает в себя программы образования, социальной интеграции и психологической поддержки [1].

Важно развивать альтернативные модели поведения и ценности, которые противостоят экстремистским идеологиям [2].

Терроризм не знает границ, поэтому эффективная борьба с ним требует международного взаимодействия. Страны должны обмениваться информацией о террористических угрозах, проводить совместные операции и разрабатывать общие стратегии.

Участие в международных организациях и соглашениях позволяет укрепить правовые рамки для борьбы с терроризмом [3].

Внедрение современных технологий, таких как системы видеонаблюдения, биометрические данные и аналитика больших данных, может значительно повысить уровень безопасности и помочь в предотвращении террористических актов [4].

Однако важно сбалансировать использование технологий с соблюдением прав человека и личной свободы граждан, способности эффективно реагировать на вызовы.

Национальная антитеррористическая безопасность требует комплексного подхода, который сочетает профилактические меры, международное сотрудничество, современные технологии и активное участие общества. Только так можно создать эффективную систему, способную защитить страну от террористических угроз и обеспечить безопасность ее граждан [5].

#### СПИСОК ЛИТЕРАТУРЫ

1. Чернядзе Н. А. Международный терроризм: происхождение, эволюция, актуальные вопросы правового противодействия: монография / Н. А. Чернядзе. Москва: Проспект, 2017// URL: <https://cyberleninka.ru/article/n/ponyatie-mezhdunarodnyy-terrorizm-v-mezhdunarodnyh-soglasheniyah-oon> (дата обращения: 25.08.2025).
2. Федеральный закон от 6 марта 2006 г. №35-ФЗ «О противодействии терроризму»// URL: <https://www.kremlin.ru/acts/bank/23522> (дата обращения: 25.08.2025).
3. Мароренко С. А. Система обеспечения антитеррористической безопасности в Российской Федерации // Вестник науки. 2023. № 6 (63). С. 553-560 // URL: <https://cyberleninka.ru/article/n/sistema-obespecheniya-antiterroristicheskoy-bezopasnost-v-rossiyskoy-federatsi> (дата обращения: 25.08.2025).
4. Бабаева Я. Г. Прокурорский надзор в сфере противодействия распространению терроризма // URL: <https://cyberleninka.ru/article/n/prokurorskiy-nadzor-v-sfere-protivodeystviya-rasprostraneniyu-terrorizma> (дата обращения: 25.08.2025).
5. Указ Президента РФ от 2 июля 2021 г. №400 «О стратегии национальной безопасности Российской Федерации»// URL: <https://www.kremlin.ru/acts/bank/47046> (дата обращения: 25.08.2025).

УДК 004

### ПРАВОВЫЕ ПРОБЛЕМЫ И ОРГАНИЗАЦИОННО-ТЕХНОЛОГИЧЕСКИЕ ОСОБЕННОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЧАСТНЫХ ВИРТУАЛЬНЫХ СЕТЕЙ

Антонова Дарья Антоновна, Шилков Владимир Ильич

Уральский федеральный университет имени первого Президента России Б.Н. Ельцина

Мира, ул., 19, Екатеринбург, 620062, Россия

e-mails: Antonova.Daria@urfu.me, vi.shilkov@urfu.ru

**Аннотация.** Обсуждаются правовые, организационные, технологические особенности и проблемы информационной безопасности, возникающие в связи с использованием частных виртуальных сетей на территории Российской Федерации. Обозначены риски и угрозы для безопасности личности и государства.

**Ключевые слова:** частная виртуальная сеть; риски; информационная безопасность; протоколы; экстремизм.

### LEGAL PROBLEMS AND ORGANIZATIONAL AND TECHNOLOGICAL FEATURES OF INFORMATION SECURITY OF PRIVATE VIRTUAL NETWORKS

Antonova Daria, Shilkov Vladimir

Ural Federal University, named after the First President of Russia B.N. Yeltsin

19 Mira St, Yekaterinburg, 620062, Russia

e-mails: Antonova.Daria@urfu.me, vi.shilkov@urfu.ru

**Abstract.** The legal, organizational, technological features and problems of information security arising in connection with the use of private virtual networks on the territory of the Russian Federation are discussed. The risks and threats to the security of individuals and the state are outlined.

**Keywords:** private virtual network; risks; information security; protocols; extremism.

Необходимость создания сетей, защищенных от постороннего вмешательства, привела к появлению ряда технологических решений, позволяющих обеспечивать сетевые соединения поверх другой сети и получивших обобщенное название виртуальной частной сети или VPN (Virtual Private Network). Виртуальные частные сети применяются организациями для установления защищённых соединений между удалёнными офисами и партнёрскими структурами. Они функционируют поверх существующих коммуникационных каналов, предоставляемых телекоммуникационными операторами, интернет-провайдерами и формируют единую логическую сеть, обеспечивая между каждой парой узлов зашифрованный канал передачи данных, который гарантирует безопасность и конфиденциальность информации.

Актуальность и необходимость исследования и анализа состояния, проблем, возможных перспектив применения виртуальных частных сетей обусловлена целым рядом причин, к которым, в частности, следует отнести не только востребованность и широкое распространение технологии VPN, но и различные технические, правовые, социально-экономические и психологические проблемы, неожиданно последовавшие вслед за появлением этой технологии.

Востребованность этой технологии подтверждается сведениями, приведенными в [1], согласно которым, к 2022 году глобальная аудитория интернет-пользователей превысила 5 миллиардов, из которых около трети пользователей активно применяют технологии частных виртуальных сетей, а пользователи из России занимают одно из лидирующих мест по числу скачиваний VPN сервисов. Актуальность исследования различных аспектов, связанных с применением этой технологии, обусловлена еще и противоречивостью мнений в оценке последствий распространения этой технологии. Так, например, в работе [2] отмечено, что «сегодня не лучшее время

использования VPN», так как абсолютная безопасность в интернете недостижима, а если будут раскрыты данные банковской карты при использовании VPN, то банк может отказаться предоставлять поддержку. В других работах, несмотря на то что авторы работ признают наличие рисков, связанных с применением технологии частных виртуальных сетей, представлены и другие точки зрения, согласно которым, применение VPN-технологий в уголовно-исполнительной деятельности открывает новые возможности для защиты данных и повышения информационной безопасности, а также повышает надежность и эффективность системы [3].

В работе [4] отмечено, что «актуально использовать VPN для собственной безопасности в России в 2023 году, в период глобальной нестабильности», несмотря на то что использование некоторых бесплатных VPN-сервисов, сохраняющих данные трафиков, является небезопасным и может наносить вред пользователям. Так, например, в соответствии с [5], VPN помогают защититься в общественных Wi-Fi сетях, скрывать IP от сайтов и провайдера. Однако скрывание IP не гарантирует анонимность, поскольку VPN-провайдеры и другие организации всё равно могут отслеживать пользователей с помощью уникальных цифровых меток, cookies и других технологий, а опасность бесплатных или условно-бесплатных VPN сервисов подтверждается случаями масштабных утечек в середине 2020 года, когда в открытом доступе было найдено свыше одного терабайта данных, включавших сведения об устройствах, пользователях и паролях. Авторы работы [6], к основным преимуществам и достоинствам виртуальных частных сетей, относят: сохранность конфиденциальной информации; наличие зашифрованного трафика, который обеспечивает защиту от прослушивания; поддержку множества протоколов; аутентификацию удаленного сайта; коммуникацию только между двумя конкретными абонентами; отсутствие задержек при обмене информацией. Однако, обращают внимание на то обстоятельство, что VPN защищает только транспортный уровень, поэтому для безопасности конечных точек необходимы шифрование данных, контроль доступа на уровне, сопоставимом с VPN-оборудованием, антивирусная защита и применение единой политики защиты во всех подключённых сетях, так как уязвимость одного узла ставит под угрозу всю систему. По мнению авторов [7], частные виртуальные сети имеют ограничения: по уязвимостям в безопасности, по штрафам за задержки при запросах, по сложности с координации с облачными инфраструктурами, по затратам на развертывание и по необходимости постоянного управления. К экономическим достоинствам относят относительно небольшие затраты на управление некоторыми VPN сетями, меньшие по сравнению с затратами на покупку защищенной «выделенной линии» у интернет-провайдера. Однако, необходимо отметить, что в ряде случаев, создание виртуальных сетей может иметь достаточно высокую стоимость, в связи с чем, применение некоторых «устаревших решений» может быть более эффективным и целесообразным. Вместе с тем, следует принять во внимание, что технология VPN, предоставляющая возможности бесконтрольной анонимной передачи информации может быть использована злоумышленниками и правонарушителями как инструмент для совершения противоправных действий, направленных против безопасности личности и государства. Так, например, к типичным угрозам, с которые могут быть реализованы злоумышленниками могут быть отнесены: призывы к экстремизму, психологическое травмирование пользователей, осуществляемое с помощью брутального контента; действия хакеров, направленные на кражи личных данных с помощью поддельных сайтов; психологические атаки со стороны манипуляторов и людей с психическими отклонениями.

Многие нерешенные вопросы, связанные с использованием VPN в России, лежат в сфере правового регулирования, так как, несмотря на принятые меры по усилению контроля за доступом к запрещённым сайтам, определённым интернет-ресурсам, социальным сетям и мессенджерам, злоумышленники продолжают использовать VPN для обхода этих ограничений и блокировок [8]. В связи с этим обстоятельством, вопросы совершенствования нормативно-правового регулирования, в частности через решения Конституционного и Верховного судов РФ, доработки законодательства и судебной практики, не теряют своей значимости и актуальности. Следует считать необходимыми и нуждающимися в постоянном уточнении как разъяснения по вопросам ответственности за нарушения, связанные с использованием VPN, так и вопросы условий применения нормативно-правовых актов, разрабатываемые с учетом мониторинга состояния и тенденций применения организационно-технологических особенностей VPN. В связи с наличием отрицательных последствий использования VPN в последние годы были предприняты конкретные меры по применению правового регулирования. Так, например, [9] ещё в 2019 году владельцев сервисов обязали подключаться к реестру запрещённых в России ресурсов. В начале 2022 года многие VPN-сервисы решили прекратить работу в России и покинули рынок, так как зарубежным провайдерам было направлено требование включить в «чёрный список» все сайты, признанные экстремистскими на территории страны. В связи с тем, что Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) получила полномочия ограничивать рекламу VPN-сервисов на территории России, были разработаны критерии для блокировки противоправных материалов. Соответствующий приказ начал действовать с 1 марта 2024 года и будет оставаться в силе до 1 сентября 2029 года [10]. В соответствии со сведениями [11], на сайте Минюста России размещён специальный реестр экстремистских материалов, включающий около 5,5 тысячи позиций.

Таким образом, на основании проведенного исследования можно сделать вывод, что в современных условиях, решения, касающиеся применения в Российской Федерации технологии VPN для создания защищенных соединений в информационных системах, относящихся к различным сферам деятельности должны

приниматься на основании комплексного анализа технических, экономических, психологических и правовых последствий этих решений.

### СПИСОК ЛИТЕРАТУРЫ

1. Дворянкин О.А. VPN технология добра или зла в современном мире. Тенденции развития науки и образования. 2022. № 90-3.
2. Купач Е.О. VPN: право на информацию или инструмент нарушения законности? // Россия в XXI веке: стратегия и тактика социально-экономических, политических и правовых реформ. Материалы XV Всероссийской научно-практической конференции студентов и молодых ученых. Барнаул, 2022. С. 172-173.
3. Лубенцов А.В., Приходько А.А. Перспективы внедрения технологий виртуальных частных сетей (VPN) в уголовно-исполнительную систему. В сборнике: Актуальные проблемы деятельности подразделений уголовно-исполнительной системы. Сборник материалов Всероссийской научно-практической конференции. В 3-х томах. Воронеж, 2024. С. 340-343.
4. Дмитриева К.Н. Преимущества и недостатки пользования услугами VPN в России // Поколение будущего: Взгляд молодых ученых-2023. Сборник научных статей 12-й Международной молодежной научной конференции. В 4-х томах. Курск, 2023.
5. Мелихова Ю.А., Анаденков Д.В. VPN и безопасность личных данных // Проблемы развития современного общества. Сборник научных статей 8-й Всероссийской национальной научно-практической конференции: в 4-х томах. Курск, 2023.
6. Горбунов К. С., Пантюхин О. И., Солодухин Б. В. Исследование решений, обеспечивающих безопасность информационных ресурсов на основе виртуальных сетей. Информационная безопасность регионов России (ИБРР-2023). И 74 XIII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 25-27 октября 2023 г.: Материалы конференции. СПОИСУ. СПб., 2023. 401 с.
7. Герлиц О.А., Попков Г.В. Выбор технологии VPN в условиях блокировок ресурсов в сети интернет. Интерэкспо Гео-Сибирь. 2022. Т. 6. С. 15-20.
8. Шоя, А. А. Правовое регулирование сервисов VPN в контексте обеспечения соблюдения баланса интересов государства, общества и отдельно взятой личности в РФ / А. А. Шоя // Международный журнал гуманитарных и естественных наук. 2024. № 10-5(97).
9. Примак Я.С. ВПН-сервисы: понятие, правовое регулирование, юридическая ответственность владельцев и пользователей виртуальных частных сетей. Наука без границ. Сборник статей Международного научно-исследовательского конкурса. Петрозаводск, 2023.
10. Тимофеев, С. В. Перспективы совершенствования Российского законодательства в области использования цифровых следов преступления / С. В. Тимофеев, Р. Х. Кочесоков // Вестник Восточно-Сибирского института МВД России. 2024. № 4(111).
11. «Штрафы за ВПН (VPN) и поиск экстремистских материалов» URL:<https://ria.ru/20250722/zakon-2029755493.html> (Дата обращения: 23.07.2025).

УДК 004.056:316.4

### СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: МЕТОДЫ, МЕХАНИЗМЫ И СПОСОБЫ МИНИМИЗАЦИИ РИСКОВ

**Бобонец Сергей Алексеевич, Сычев Сергей Евгеньевич**

ВГУЮ (РПА Минюста России)

10-я линия ВО, 19, литер А, Санкт-Петербург, 199178, Россия

e-mails: sbobon@mail.ru, s75sichev@mail.ru

**Аннотация.** Рассматриваются основные виды атак социальной инженерии (фишинг, претекстинг, байтжекинг, квэринг), их психологические механизмы, а также последствия для организаций и государственных структур. Представлены современные подходы к минимизации рисков, включая обучение персонала, внедрение политик безопасности и использование технических средств защиты. Особое внимание уделено необходимости комплексного подхода к противодействию социальной инженерии как важной составляющей общей стратегии обеспечения информационной безопасности.

**Ключевые слова:** социальная инженерия; информационная безопасность; фишинг; претекстинг; человеческий фактор; киберугрозы; кибербезопасность; защита информации.

### SOCIAL ENGINEERING AS A THREAT TO INFORMATION SECURITY: METHODS, MECHANISMS AND WAYS TO MINIMIZE RISKS

**Bobonets Sergey, Sychev Sergey**

VSUYU (RPA of the Ministry of Justice of Russia)

19, 10-th Linia, VI, letter A, St. Petersburg, 199178, Russia

e-mails: sbobon@mail.ru, s75sichev@mail.ru

**Abstract.** The main types of social engineering attacks (phishing, pretexting, baytjacking, quaring), their psychological mechanisms, as well as consequences for organizations and government structures are considered. Modern approaches to risk minimization are presented, including staff training, implementation of security policies and use of technical means of protection. Special attention is paid to the need for an integrated approach to countering social engineering as an important component of the overall information security strategy.

**Keywords:** social engineering; information security; phishing; pretexting; human factor; cyber threats; cybersecurity; information protection.

Современные системы информационной безопасности достигли высокого уровня технической защищённости благодаря развитию шифрования, многофакторной аутентификации, систем обнаружения вторжений и других технологий. Однако человеческий фактор остаётся н одним из самых уязвимых элементов в этой системе. Благодаря взаимодействию с человеком (пользователем, администратором и т.п.) злоумышленники могут получить беспрепятственный доступ к конфиденциальной информации, используя методы социальной инженерии, который заключается в искусстве манипуляции поведением и доверием людей.



Социальная инженерия представляет собой, прежде всего, не техническую, а психологическую угрозу, которая может быть реализована в любой, даже хорошо защищённой системе. Следует отметить, что успешная атака на информационные ресурсы организации не требует глубоких знаний программирования или хакерских навыков, достаточно понимания психологии жертвы и умения воспользоваться её доверием. Злоумышленники используют невнимательность и доверчивость жертвы или ее желание помочь [1].

Задача исследования современных методов и механизмов социальной инженерии, анализа их влияния на информационную безопасность, а также разработка рекомендаций по минимизации связанных с ними рисков, является актуальной.

Механизмы социальной инженерии базируются на методах получения конфиденциальной информации или несанкционированного доступа к защищённым системам путём психологического воздействия на человека. Задача злоумышленника не искать уязвимости в коде, а организовать психологическое воздействие на сознание и поведение пользователя [2, 3].

Практика применения методов социальной инженерии известна давно, хотя сам термин «социальная инженерия» был впервые использован в 90-х годах XX века. Примеры манипуляционного воздействия на человека можно найти издревле, мошенники во все времена пользовались этими методами. В современном мире, когда информационно-коммуникационные технологии проникли во все сферы человеческой деятельности, формы социальной инженерии значительно изменились, т.к. появился интернет и цифровые коммуникации. Теперь злоумышленник может организовать дистанционное психологическое воздействие, не общаясь с жертвой глаза в глаза. Интернет и цифровые коммуникации вывели социальную инженерию на новый уровень [4].

При психологическом воздействии на жертву, основными целями социальной инженерии являются [2]:

- получение логина и пароля доступа к информационным ресурсам, особенно с правами администратора;
- доступ к ресурсам внутренней корпоративной сети;
- получение конфиденциальной информации, в том числе финансовой и ограниченного распространения;
- вербовка сотрудников организации (подкуп, шантаж и т.п.);
- внедрение вредоносного программного обеспечения.

Существуют различные методы и типы атак социальной инженерии, рассмотрим основные из них [5, 6, 7]:

- Фишинг (Phishing) — отправка поддельных писем, сообщений, запросов, имитирующих официальные письма от руководителей организации, банков, сервисов, коллег. Целью таких действий является получение логинов, паролей, данных банковских карт и специальных сведений для доступа к ресурсам. Как правило, фишинг ассоциируется с рассылками по электронной почте, но существуют и подвиды: смсшинг — фишинг через SMS; вишинг — через телефонный звонок; spear phishing — персонализированный фишинг.

- Претекстинг (Pretexting) — вовлечение пользователя в решение ситуационной задачи. Злоумышленник создает вымышленную ситуацию (например, проблемы с оборудованием, проблемы с сетевым подключением, проверка аккаунта, опрос, техподдержка и т.п.) и запрашивает информацию, необходимую для совершения атаки.

- Байтжекинг (Baiting) — провокация любопытства, когда злоумышленник в общественном месте оставляет USB-накопитель или мобильное периферийное устройство, которое затем используется для установки вредоносного программного обеспечения на компьютер жертвы.

- Квэринг (Quid Pro Quo) — услуга или подарок в обмен на предоставление данных или выполнение определённых действий.

- Тейлгейтинг (Tailgating) — физическое вторжение в защищённое помещение вслед за сотрудником без предъявления пропуска, используется такое понятие как «вход на плечах».

Помимо описанных выше методов, существуют психологические механизмы социальной инженерии [1, 2].

- Принцип доверия — склонность доверять знакомым брендам, компаниям, лицам, представляющимся сотрудниками службы поддержки, курьерам, банковским работникам, сотрудникам правоохранительных органов.

- Стресс и спешка — лимит времени или стрессовая ситуация заставляет пользователя принимать решения игнорируя стандартные процедуры проверки безопасности.

- Авторитетность — обращение от имени руководителя или авторитетного лица снижает бдительность пользователя и вызывает автоматическое исполнение указаний.

- Стремление помочь — желание быть полезным, особенно у малоопытных сотрудников, делает их уязвимыми перед атаками.

- Информационная и эмоциональная перегрузка — чрезмерный поток информации и прессинг снижает внимательность и критическое мышление, что увеличивает вероятность ошибки.

Социальная инженерия оказывает негативное воздействие на информационную безопасность и увеличивает риск утечки персональных и корпоративных данных. Убытки от успешных атак могут быть значительными, особенно если затронуты персональные данные пользователей или технологические процессы.

Государственные организации и критическая инфраструктура также подвержены атакам, что может привести к негативным последствиям и нанести значительный ущерб репутации. Организации, столкнувшиеся с утечкой данных, сталкиваются с потерей доверия клиентов и партнёров [8].

С целью противодействия методам социальной инженерии необходим комплексный подход, который должен включать: обучение и повышение осведомлённости, формирование политики безопасности, использование технических решений, аудит, тестирование и четкость процедур верификации.

Таким образом, социальная инженерия остаётся одной из самых опасных и недооценённых угроз в сфере информационной безопасности. Её эффективность основана на психологических особенностях человека, что делает традиционные технические средства недостаточными для полноценной защиты. Для противодействия таким атакам необходимо внедрять комплексный подход, объединяющий обучение персонала, политики безопасности и технические меры. Только сочетание всех этих компонентов позволит снизить уровень риска и повысить устойчивость организаций к психологическим атакам в цифровом пространстве.

#### СПИСОК ЛИТЕРАТУРЫ

1. Логунова, О. С. Информационная безопасность: социально-психологические аспекты / О. С. Логунова. Москва : Академия, 2020. 256 с.
2. Алексеев, А. Н. Социальная инженерия: психологические аспекты киберугроз : монография / А. Н. Алексеев, И. А. Михайлов. Москва: Инфра-М, 2021. 180 с.
3. Хорошев, А. А. Киберугрозы и способы их предотвращения: от технических до психологических аспектов / А. А. Хорошев. Нижний Новгород: ННГУ, 2020. 216 с.
4. Романенко, А. В. Практическая социальная инженерия: анализ атак и методы защиты / А. В. Романенко. Москва: Эксмо, 2022. 272 с.
5. Гаврилов, А. С. Компьютерная безопасность для пользователей: от фишинга до защиты паролей / А. С. Гаврилов. Москва: ДМК Пресс, 2020. 224 с.
6. Дорофеев, А. А. Социальная инженерия в цифровой экономике: методология, методы, защита / А. А. Дорофеев. Новосибирск: НГТУ, 2022. 210 с.
7. Орехов, А. В. Социальная инженерия: угрозы и методы противодействия / А. В. Орехов, А. С. Романов. Казань: Казанский университет, 2021. 198 с.
8. Шарипов, Р. А. Социальная инженерия в сфере государственной информационной безопасности / Р. А. Шарипов. Москва: МГУ им. М. В. Ломоносова, 2021. 190 с.

УДК 004.7

#### АНОНИМНОСТЬ В СЕТИ И ЕЁ ВЛИЯНИЕ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

**Бобонец Сергей Алексеевич, Сычев Сергей Евгеньевич**

ВГУЮ (РПА Минюста России)

10-я линия ВО, 19, литер А, Санкт-Петербург, 199178, Россия

e-mails: sbobon@mail.ru, s75sichev@mail.ru

**Аннотация.** Рассматриваются современные подходы и технологии анонимного сетевого взаимодействия, такие как Tor, VPN, зашифрованные мессенджеры, а также их влияние на информационную безопасность. Анализируется двойственная роль анонимности в сетевом пространстве. С одной стороны, анонимность оказывает позитивное влияние на защиту личных данных, с другой стороны, имеет негативные последствия, связанные с усугублением ситуации в сфере кибербезопасности. Проанализированы вызовы, с которыми сталкиваются правоохранительные органы и специалисты по кибербезопасности при расследовании инцидентов в условиях высокой степени анонимности пользователей. На основе анализа сделан вывод о необходимости разработки комплексного подхода к обеспечению баланса между безопасностью и приватностью.

**Ключевые слова:** анонимность; информационная безопасность; кибербезопасность; Tor; VPN; деанонимизация; киберпреступность; цифровая приватность.

#### ONLINE ANONYMITY AND ITS IMPACT ON INFORMATION SECURITY

**Bobonets Sergey, Sychev Sergey**

VSUYU (RPA of the Ministry of Justice of Russia)

19, 10-th Linia, VI, letter A, St. Petersburg, 199178, Russia

e-mails: sbobon@mail.ru, s75sichev@mail.ru

**Abstract.** Modern approaches and technologies of anonymous network interaction, such as Tor, VPN, encrypted messengers, as well as their impact on information security, are considered. The dual role of anonymity in the online space is analyzed. On the one hand, anonymity has a positive impact on the protection of personal data, on the other hand, it has negative consequences related to the aggravation of the situation in the field of cybersecurity. The challenges faced by law enforcement agencies and cybersecurity specialists in investigating incidents under conditions of high user anonymity are analyzed. Based on the analysis, it is concluded that it is necessary to develop an integrated approach to ensuring a balance between security and privacy.

**Keywords:** anonymity; information security; cybersecurity; Tor; VPN; deanonymization; cybercrime; digital privacy.

Анонимность в сетевом пространстве представляет собой важную и многогранную концепцию, которая в последнее время стала объектом активного изучения [1, 2]. Связано это с двойственным пониманием анонимности, что приводит к её различным интерпретациям в контексте информационной безопасности. С одной стороны, она выступает важным инструментом защиты приватности, свободы слова и прав человека, а с другой — создаёт условия для совершения киберпреступлений, распространения дезинформации и организации противоправной деятельности.

С развитием цифровых технологий проблема обеспечения информационной безопасности становится всё более сложной и многогранной. Рост уровня анонимности в интернете является ключевым фактором, влияющим на ситуацию в сфере кибербезопасности. Соккрытие реальной идентичности пользователя и его фактического местоположения открывает новые возможности для реализации незаконных действий и возможного ухода от ответственности [3, 4].

Значение анонимности возрастает в связи с увеличением числа пользователей, желающих сохранить конфиденциальность своих действий в цифровом пространстве. При этом анонимность стала не просто технической особенностью использования интернета, но и объектом внимания со стороны государственных структур, частных компаний, правозащитников и специалистов кибербезопасности [5].

Анализ роли анонимности в сфере информационной безопасности направлен на исследование её положительного и отрицательного влияния, а также выявление актуальных вызовов и перспектив развития в контексте обеспечения баланса между безопасностью и приватностью.

Анонимность в интернете, связанная с желанием пользователя скрывать свою идентичность, местоположение и поведение в цифровом пространстве, может быть достигнута различными способами: использование псевдонимов, применение программных решений, маскирующих IP-адрес, или работа через защищённые сети [6].

Классифицировать анонимность можно по типам: полная, ограниченная и псевдоанонимность. Также различают добровольную и вынужденную анонимность. Первый тип используется с целью защиты личной информации, второй — применяется в ситуациях, связанных с политическим давлением, цензурой или угрозами.

К современным технологиям, обеспечивающим анонимность, следует отнести [7]:

- Tor (The Onion Router) — система маршрутизации трафика, которая использует принцип многослойного шифрования.

- VPN-сервисы позволяют создавать защищённое соединение между пользователем и сервером провайдера, что позволяет скрыть реальный IP-адрес и обеспечивает защиту данных от прослушивания третьими лицами.

- Шифрованные мессенджеры — используют сквозное шифрование, гарантирующее, что только отправитель и получатель могут прочесть сообщение.

- Приватные поисковые системы — не собирают данные о пользователях, что делает их предпочтительным выбором для тех, кто заботится о своей цифровой приватности.

Анонимность оказывает положительное влияние на информационную безопасность, это связано, прежде всего, с защитой личных данных, обеспечением свободы слова, укреплением доверия к цифровому пространству, предотвращением цензуры и слежки [8, 9].

Вместе с тем, анонимность оказывает и негативное влияние на информационную безопасность. Это связано с возможностью сокрытия киберпреступлений, распространением дезинформации и фейков, пропагандой негативных ценностей, радикализацией и экстремизмом [2 — 4]. Правоохранительные органы сталкиваются с проблемами в расследовании киберпреступлений, особенно если серверы, через которые действуют злоумышленники, находятся вне юрисдикции страны.

Современные цифровые технологии не стоят на месте и развивают подходы к деанонимизации. Для противодействия злоупотреблениям анонимностью разрабатываются:

- методы и способы анализа метаданных;
- инструментальные методы машинного обучения для выявления подозрительной активности;
- системы распределённого наблюдения и анализа трафика.

Отдельно следует отметить, что такие меры должны применяться строго в рамках закона и с соблюдением этических норм [5, 8].

Таким образом, анонимность в сети представляет собой сложный и многогранный процесс, который одновременно может служить защитой для пользователей и создавать новые риски для информационной безопасности. Решение проблем анонимности в цифровом пространстве требует комплексного подхода, сочетающего технические решения, правовое регулирование и этические принципы. Соблюдение баланса между необходимостью обеспечения приватности и защитой от киберугроз, окажет положительное влияние на развитие цифрового общества будущего.

#### СПИСОК ЛИТЕРАТУРЫ

1. Шарков, А. В. Анонимность в Интернете: лица и инструменты // Безопасность информационных технологий, 2021.
2. Митрофанов, А. С. Проблемы анонимности в интернете: взгляд на безопасность // Известия высших учебных заведений. Серия: Прикладная и профессиональная деятельность в сфере информационных технологий, 2019.
3. Загороднюк, И. В. Кибербезопасность и анонимность: положительные и отрицательные аспекты. Журнал Информационная безопасность, 2020.
4. Баранов, В. С. Анонимность и безопасность в киберпространстве: вызовы и риски. Журнал Компьютерные исследования и разработки, 2021.
5. Павлов, И. Н. Анонимность в интернете и её влияние на социальные взаимодействия // Современные проблемы науки и образования, 2020.
6. Савельев, Д. А. Анонимные инструменты: как они влияют на информационную безопасность в России. Вестник информационных технологий, 2022.
7. Доронин, Е. В. Тор, VPN и другие способы анонимизации: технологии и риски. Научно-аналитический журнал Кибербезопасность, 2022.
8. Кузнецова, М. Р. Влияние анонимности на свободу слова и киберугрозы. Научные труды Института права и публичной политики, 2019.
9. Емельянов, А. Г. Анонимные сети как инструмент защиты личных данных // Безопасность и информационные технологии, 2020.

УДК 004; 519

**АЛГОРИТМ ОЦЕНКИ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СИСТЕМЫ ПОЖАРНОЙ СИГНАЛИЗАЦИИ ПРИ УПРАВЛЕНИИ СИСТЕМАМИ ПОЖАРНОЙ АВТОМАТИКИ****Богущий Сергей Юрьевич<sup>1</sup> Синешук Юрий Иванович<sup>2</sup>**<sup>1</sup> ФГБУ СЭУ ФПС ИПЛ по г. Санкт-Петербургу

Пеньковская ул., 6, Санкт-Петербург, 197046, Россия

<sup>2</sup> Санкт-Петербургский университет ГПС МЧС России

Московский пр., 149, Санкт-Петербург, 196105, Россия

e-mails: bsu-01@yandex.ru, sinegal53@mail.ru

**Аннотация.** Предложена информационно-логическая модель системы пожарной сигнализации и разработан алгоритм оценки функциональной безопасности и сравнительных оценок различных инженерных решений систем пожарной сигнализации при выполнении функций управления.

**Ключевые слова:** система противопожарной защиты; система пожарной автоматики; система пожарной сигнализации; функция безопасности; функция управления.

**ALGORITHM FOR ASSESSING THE FUNCTIONAL SAFETY OF A FIRE ALARM SYSTEM WHEN CONTROLLING FIRE AUTOMATION SYSTEMS****Bogutsky Sergey<sup>1</sup>, Sineshchuk Yuriy<sup>2</sup>**<sup>1</sup> Federal State Budgetary Institution of the Russian Federation «SEU FPS IPL» for the city of St. Petersburg

6 Penkova St, St. Petersburg, 197046, Russia

<sup>2</sup> St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia

149 Moskovskiy Av, St. Petersburg, 196105, Russia

e-mails: bsu-01@yandex.ru, sinegal53@mail.ru

**Abstract.** An information-logical model of a fire alarm system is proposed and an algorithm for assessing the functional safety and comparative assessments of various engineering solutions for fire alarm systems when performing control functions is developed.

**Keywords:** fire protection system; fire automation system; fire alarm system; safety function; control function.

Снижение воздействия опасных факторов пожара на людей и материальные ценности достигается применением систем пожарной автоматики (СПА), предназначенных для смягчения последствий опасного события — пожара, снижая риски путем уменьшения тяжести последствий. Эти обстоятельства позволяют отнести реализуемый СПА функционал к функциям безопасности [1, 2]. Особую, системообразующую роль играет система пожарной сигнализации (СПС). В большинстве случаев, помимо функции обнаружения пожара, СПС должна обеспечивать выдачу сигналов управления на другие системы СПА. Эти особенности СПС позволяют признать одной из важнейших характеристик ее функциональную безопасность, которая определяется как составная часть (элемент) системной безопасности. При анализе надежности систем, связанных с безопасностью, вместо вероятности отказа используется понятие «вероятность отказа при наличии запроса», т.е. вероятность отказа при наличии необходимости быть в состоянии готовности [3].

Среднюю вероятность отказа по запросу для функции безопасности системы будем оценивать посредством определения и суммирования средних вероятностей отказов по запросу для всех подсистем, которые реализуют конкретную функцию безопасности. Специально для целей проведения исследования, предлагается воспользоваться информационно-логическими моделями СПА, в части выполнения и отказа выполнения функции безопасности, при обеспечении функции управления. Следует обратить внимание, что в различных зонах объекта защиты могут применяться элементы с различными показателями интенсивности отказов, а сами подсистемы могут быть различных архитектур [4, 5].

Предложенный алгоритм реализован в виде специального программного обеспечения, позволяющего проводить автоматизированную, многовариантную оценку функциональной безопасности как с учётом архитектуры составляющих её отдельных подсистем и надёжности их компонентов, так и параметров, определяющих процесс её эксплуатации при проведении периодических технических обслуживаний, а также анализ различных инженерных решений в части обеспечения выполнения требуемых функций безопасности на различных этапах жизненного цикла.

**СПИСОК ЛИТЕРАТУРЫ**

1. Соколов С. В., Костюченко Д. В. Эффективность средств пожарной автоматики на пожарах в жилых домах. Пожаровзрывобезопасность. 2014. Т. 23, № 6. С. 70–75.
2. Kubica Przemysław, Wnęk Waldemar, Boroń Sylwia// Selected principles of developing fire scenarios// CNBOP-PIB. 2016. BitP Vol. 42 I. 2, 2016, pp. 173–178.
3. Зыков П. И. О расчете вероятности эффективной работы технических средств по обеспечению пожарной безопасности при определении расчетных величин пожарного риска на производственных объектах. // Техносферная безопасность №4. 2021. С.67-71.
4. Богущий С.Ю., Синешук Ю.И. Метод оценки функциональных характеристик систем пожарной автоматики многоквартирных жилых домов. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2024. № 2. С. 11–22.
5. Богущий С.Ю., Синешук Ю.И. Методика оценки функциональной безопасности системы пожарной сигнализации на основе информационно-логической модели. Проблемы управления рисками в техносфере. 2025. № 2 (74). С. 118-129.

УДК 37.091.315.7

**ПРИМЕНЕНИЕ СПЕЦИАЛИЗИРОВАННЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ ДЛЯ ПОВЫШЕНИЯ  
ЭФФЕКТИВНОСТИ ПРОВЕДЕНИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ С КУРСАНТАМИ  
ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИ ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ  
РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Гармаев Амгалан Алдарович, Марков Дмитрий Алексеевич**

Академия войск национальной гвардии

Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия

e-mails: amgalan5273@mail.ru, markovDA@mail.ru

**Аннотация.** В данной статье рассматривается методика применения инновационных технологий для эффективного достижения целей занятий в достаточно непростых вопросах математического анализа.

**Ключевые слова:** Mathcad; математические пакеты; символьные вычисления.

**THE USE OF SPECIALIZED COMPUTER PROGRAMS TO IMPROVE THE EFFECTIVENESS  
OF PRACTICAL TRAINING FOR CADETS OF EDUCATIONAL INSTITUTIONS  
OF THE RUSSIAN FEDERATION NATIONAL GUARD TROOPS**

**Garmaev Amgalan, Markov Dmitry**

Academy of the National Guard Troops

1 Pilot Pilyutova St, St. Petersburg, 198206, Russia

e-mails: amgalan5273@mail.ru, markovDA@mail.ru

**Abstract.** This article discusses the application of innovative technologies to effectively achieve the goals of classes in rather complex issues of mathematical analysis.

**Keywords:** Mathcad; mathematical packages; symbolic calculations.

В соответствии с учебными планами подготовки курсантов образовательных организаций войск национальной гвардии Российской Федерации по разным направлениям обучения, изучается ряд дисциплин, у которых практические занятия непосредственно связаны с применением информационных технологий. К ним относятся: математика; физика; начертательная геометрия, инженерная и компьютерная графика и др.

На сегодняшний день существует несколько математических пакетов, с помощью которых быстро, просто и эффективно выполняются сложные математические расчеты, причем даже в символьном виде. Здесь следует обратить внимание на такие средства вычислений, как Maple, Mathematica и Mathcad. Пакеты эти выделены именно потому, что в них на достаточно серьезном уровне поддерживаются символьные вычисления. Что касается пакета Mathcad, то в нем символьные вычисления являются скорее данью моде и ответом на современные вызовы рынка. Однако, это ни в коей мере не умаляет возможностей Mathcad, скорее наоборот. Он неизменно популярен, особенно среди студентов (курсантов) и инженеров (по-видимому, в силу простоты взаимодействия пользователя с приложением и прозрачности выполняемых операций). Возможности приложения постоянно расширяются, в силу чего Mathcad все чаще используется не только в физико-инженерных расчетах, но и при решении задач экономики, в финансовых расчетах, в социологии и биологии (список можно продолжить) [1].

Методика сводится к выполнению курсантами предложенных заданий, предполагающих как расчет, так и символьные преобразования предложенных функций (при проведении дифференциальных и интегральных вычислений) с последующей проверкой результата в среде интегрированного пакета MathCad. При проведении практических занятий курсанты на первом этапе самостоятельно осуществляют решение задачи (без применения пакета MathCad), целесообразно, на этом этапе применять элемент «соревновательности», «соперничества» между курсантами. Первый, кто выполнит предложенное задание, имеет возможность, проверив его в интегрированном пакете MathCad, приступить к выполнению следующей задачи. Таким образом, при использовании данной методики налицо применение интерактивной технологии обучения: самостоятельное решение задач, проверка ее решения и переход к выполнению следующего этапа задачи [2].

Целесообразно применить вышеизложенную методику в процессе обучения курсантов, как под руководством преподавателя, так и в часы самостоятельной подготовки, что существенно повышает эффективность форм обучения.

Кроме этого, опыт проведения практических занятий с применением интегрированного пакета MathCad позволяет сделать вывод об эффективности освоения изучаемого материала при этом понимании «физики процесса» существенно повышается.

Интегрированный пакет MathCad позволяет визуализировать излагаемый материал. Например, в разделе «Основы математической статистики», понимание курсантами того, что такое «функция распределения случайной величины», «плотность распределения», какова связь между этими функциями, способ проверки полученного результата осуществляется достаточно оперативно и наглядно (в частности, нахождение площади фигуры под графиком плотности распределения, которая должна равняться единице, легко проверяется средствами интегрированного пакета MathCad посредством операции интегрирования указанной функции) [3].

Таким образом, представленная выше методика применения инновационных технологий, интерактивный подход (теория — практика — теория) в процессе изучения вопросов математической направленности, позволяет

эффективно достичь цели занятия — разобраться в достаточно непростых вопросах математического анализа основ статистики и применить их в практической плоскости.

#### СПИСОК ЛИТЕРАТУРЫ

1. Глотова М.И., Приходько О.В. Основы работы в среде MathCAD. Простейшие вычисления. Часть 1. Оренбург: 2013.
2. Алябьева С.В., Борматова Е.П., Данилова М.В., Семёнова Е.Е. «MathCAD для студентов» Учебный практикум. Петрозаводск: ПетрГУ. 2007.
3. Матвейкина В.П. Применение информационных технологий в преподавании математики // «Перспективы развития информационных технологий» №19. 2014.

УДК 004

### ПЕРЕХОД С ЗАПАДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА ОТЕЧЕСТВЕННОЕ КАК ФАКТОР ПОВЫШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Грacheв Михаил Иванович**

Санкт-Петербургский университет МВД России  
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия  
e-mail: mig2500@mail.ru

**Аннотация.** В условиях геополитической нестабильности и роста числа киберугроз использование западного программного обеспечения (ПО) создаёт дополнительные риски для информационной безопасности (ИБ) предприятий и государственных структур. Предлагается модель управления переходом на отечественные программно-аппаратные комплексы (ПАК) на основе модели решения человека позволяющей принимать во внимание анализ состояния системы, а также применять решение обратной задачи для распределения ресурсов. Показано, что применение отечественного ПО в сочетании с кадровыми и организационными мерами снижает вероятность критических инцидентов, повышая эффективность управленческих процессов.

**Ключевые слова:** информационная безопасность; импортозамещение; отечественное программное обеспечение; оптимизация ресурсов; киберугрозы; технологический суверенитет.

### TRANSITION FROM WESTERN TO DOMESTIC SOFTWARE AS A FACTOR IN INCREASING INFORMATION SECURITY

**Grachev Mikhail**

St. Petersburg University of the Ministry of Internal Affairs of Russia  
1 Pilot Pilyutova St, St. Petersburg, 198206, Russia  
e-mail: mig2500@mail.ru

**Abstract.** In the context of geopolitical instability and the growth of cyber threats, the use of Western software creates additional risks for the information security of enterprises and government agencies. A management model for the transition to domestic hardware and software systems (HSS) is proposed based on a human decision model that allows taking into account the analysis of the system state, as well as applying the solution of the inverse problem for resource allocation. It is shown that the use of domestic software in combination with personnel and organizational measures reduces the likelihood of critical incidents, increasing the efficiency of management processes.

**Keywords:** information security; import substitution; domestic software; resource optimization; cyber threats; technological sovereignty.

В условиях геополитической нестабильности и усиления киберугроз, вопрос перехода на отечественное программное обеспечение приобретает стратегическое значение для обеспечения национальной безопасности [1-4].

Комплексный подход к миграции, включающий в себя анализ текущей инфраструктуры, определение приоритетных направлений и разработку детального плана внедрения, является залогом успешной реализации проекта. Переход на отечественное ПО — ключевой элемент технологического суверенитета и устойчивости предприятий. Использование зарубежных ИТ-продуктов сопряжено с рисками: удалённым управлением лицензиями, ограничениями в обновлениях, возможными закладками в коде. Комплексная замена западных решений требует технической, кадровой и организационной подготовки [5].

Успешная миграция на отечественное ПО — это не просто замена одного продукта на другой, а комплексная трансформация, направленная на повышение эффективности и безопасности информационных систем. Это инвестиция в будущее, обеспечивающая технологическую независимость и устойчивое развитие в условиях быстро меняющегося мира. Важным аспектом является выбор отечественных решений, соответствующих требованиям безопасности и функциональности. Проведение тщательного тестирования и пилотных проектов позволяет оценить возможности программного обеспечения в реальных условиях и адаптировать его под специфические потребности организации.

Каждый руководитель предприятия за годы своей работы накопил бесценный опыт, который со временем формируется в последовательную модель выполняемых действий для преодоления тех или иных трудностей возникающих по ходу работы предприятия. Данный факт о модельном представлении мышления в своих работах указывал академик П.К. Анохин [6].

В работах других авторов модель решения человека рассматривается как решение прямой задачи по достижению цели деятельности, что не всегда гарантирует требуемый результат. Данный факт, подтверждается отсутствием в литературных источниках модели позволяющей гарантированно достигать цели деятельности. Для решения данной задачи можно использовать системообразующий фактор, в основе которого лежит естественно-научный подход позволяющий получить условие существования процесса управления. Получив условие существования процесса управления можно применять математическое моделирование, основанное на связи целевого процесса, процесса возникновения трудностей, процесса определения трудностей и процесса нейтрализации трудностей. Данная постановка вопроса позволяет рассматривать получаемую модель как систему увязывающую человеко-машинную систему, в состав которой входят и ресурсы, которыми располагает руководитель организации [7].

Модель позволит оценить имеющуюся систему и в дальнейшем на основе определения изъянов в предприятии устранить их за счет применения резервов, которыми располагает руководитель предприятия. После применения полученной математической модели можно применять комбинированные решения перехода.

В общем виде модель перехода на отечественное ПО можно представить в следующем виде:

- штатная работа — функционирование системы на отечественном ПО без сбоев;
- выявление уязвимости — оценка потенциальных рисков при использовании западных решений;
- переходный этап — параллельное функционирование старых и новых систем;
- полная миграция — завершённый переход и интеграция отечественных решений в инфраструктуру.

Данное направление перехода из западного ПО на отечественное сопряжено с необходимостью моделирования различных ресурсов: технических — внедрение отечественных ПАК, систем управления базами данных, офисных пакетов и средств шифрования; кадровых — обучение персонала работе с отечественными продуктами, формирование экспертных групп поддержки; финансовых — планирование затрат на миграцию и сопровождение; организационных — регламентированное управление изменениями, имитационное моделирование рисков.

Эффективное распределение ресурсов предполагает не только финансовые инвестиции, но и оптимизацию трудозатрат, обучение персонала и использование инструментов автоматизации. Грамотное планирование и управление проектом позволяют минимизировать риски возникновения проблем совместимости, простоев в работе и снижения производительности.

Для реализации модели должны в приоритете применяться отечественное ПО в критически важных системах. Должна разрабатываться поэтапная миграция с минимизацией простоев. Необходимо создание центров компетенций по отечественным ИТ-решениям. Проведение интеграции средств мониторинга и защиты, полностью контролируемых внутри страны.

Данная совокупность факторов позволит снизить вероятность критических инцидентов, повышая эффективность управленческих процессов.

Переход на отечественное ПО повышает устойчивость информационной инфраструктуры, снижает риски внешнего воздействия и обеспечивает независимость критических процессов от иностранных поставщиков. Решение задачи оптимального распределения ресурсов в процессе миграции позволяет достичь максимальной эффективности при минимальных издержках и временных затратах.

#### СПИСОК ЛИТЕРАТУРЫ

1. Полонский, А. М. Импортзамещение программного обеспечения и организация обучения студентов с использованием отечественного или свободного программного обеспечения // Актуальные проблемы экономики и управления. 2022. № 2(34). С. 65-82. EDN YMGTXU.
2. Киселев, Д. А. Импортзамещение иностранного программного обеспечения в задаче обеспечения безопасности информационных ресурсов исполнительных органов власти / Д. А. Киселев // Научный аспект. 2023. Т. 2, № 11. С. 183-188. EDN VOXXFZ.
3. Лукичев, С. В. Развитие отечественного программного обеспечения это не только решение задачи импортзамещения, но и обеспечения технологической независимости страны / С. В. Лукичев // Горная промышленность. 2022. № 2. С. 12-14. EDN MOVTNN.
4. Пасурин, Д. А. Проблемы импортзамещения программного обеспечения в вузе / Д. А. Пасурин // Цифровые модели и решения. 2023. Т. 2, № 4. С. 63-75. DOI 10.29141/2949-477X-2023-2-4-6. EDN JBUIWS.
5. Грачев, М. И. Комплексный подход к безопасности предприятия включая имитационное моделирование / М. И. Грачев, Н. Г. Грачева // Информационная безопасность регионов России (ИБРР-2023): XIII Санкт-Петербургская межрегиональная конференция. Материалы конференции, Санкт-Петербург, 25–27 октября 2023 года. Санкт-Петербург: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2023. С. 74-75. EDN JSKVCD.
6. Анохин, П. К. Идеи и факты в разработке теории функциональных систем // Психологический журнал. 1984. Т. 5. С. 107-118.
7. Грачев, М. И. Математическое моделирование в социальных и экономических системах / М. И. Грачев, В. Г. Бурлов // T-Comm: Телекоммуникации и транспорт. 2021. Т. 15. № 5. С. 38-45.

УДК 378.147

#### ПОДГОТОВКА КУРСАНТОВ И СЛУШАТЕЛЕЙ СИСТЕМЫ МВД РОССИИ

Грачева Наталья Геннадьевна

Санкт-Петербургский университет МВД России

Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия

e-mail: kng25@list.ru

**Аннотация.** Современная профессиональная подготовка и морально-психологическое обеспечение (МПО) курсантов и слушателей МВД России требуют интеграции сетевых технологий взаимодействия.

В условиях цифровизации образовательной и служебной среды актуализируются задачи обеспечения информационной безопасности (ИБ) и сохранения психологической устойчивости обучающихся. Необходим комплексный подход, учитывающий специфику ведомственного образования, риски киберсреды и требования к формированию профессионально значимых качеств сотрудников правоохранительных органов.

**Ключевые слова:** сетевое взаимодействие; профессиональная подготовка; морально-психологическое обеспечение; курсанты МВД; информационная безопасность; киберугрозы; психологическая устойчивость; дистанционное обучение; ведомственное образование.

## TRAINING OF CADETS AND STUDENTS OF THE SYSTEM OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA

Gracheva Natalia

St. Petersburg University of the Ministry of Internal Affairs of Russia

1 Pilot Pilyutova St, St. Petersburg, 198206, Russia

e-mail: kng25@list.ru

**Abstract.** Modern professional training and moral-psychological support (MPS) of cadets and students of the Russian Ministry of Internal Affairs (MIA) require the integration of network interaction technologies. In the context of digitalization of the educational and service environment, the tasks of ensuring information security (IS) and maintaining the psychological resilience of students become paramount. An integrated approach is needed that considers the specifics of departmental education, the risks of the cyber environment, and the requirements for the formation of professionally significant qualities of law enforcement officers.

**Keywords:** network interaction; professional training; moral-psychological support; MIA cadets; information security; cyber threats; psychological resilience; distance learning; departmental education.

Активное внедрение цифровых платформ, систем дистанционного обучения и сетевых коммуникаций в образовательный процесс и служебную деятельность системы МВД России создает новые возможности для профессиональной подготовки и морально-психологического обеспечения (МПО) курсантов и слушателей [1, 2].

Уникальность контингента — будущих сотрудников правоохранительных органов — предъявляет повышенные требования к защите данных, конфиденциальности служебной информации и сохранению их морально-психологической устойчивости в условиях киберугроз [3].

В этой связи, образовательные учреждения, готовящие кадры для правоохранительных органов, сталкиваются с необходимостью разработки и внедрения комплексных мер по обеспечению кибербезопасности и защите персональных данных курсантов и слушателей.

Эти меры должны охватывать не только технические аспекты, такие как защита сетей и систем от несанкционированного доступа, но и обучение будущих сотрудников основам информационной безопасности, кибергигиены и противодействия социальным инженерным атакам.

Особое внимание следует уделять формированию у курсантов и слушателей навыков критического мышления и умения распознавать признаки деструктивного информационного воздействия.

Важно научить их анализировать информацию, поступающую из различных источников, выявлять фейки и пропаганду, а также противостоять манипуляциям и попыткам вовлечения в противоправную деятельность в сети Интернет [4].

Кроме того, необходимо разрабатывать и внедрять программы психологической поддержки и реабилитации для сотрудников, столкнувшихся с киберугрозами или ставшими жертвами киберпреступлений. Такие программы должны быть направлены на восстановление морально-психологической устойчивости, снижение уровня стресса и тревожности, а также на формирование у сотрудников навыков эффективного преодоления негативных последствий кибервоздействия.

Таким образом, обеспечение кибербезопасности и защита персональных данных будущих сотрудников правоохранительных органов является комплексной задачей, требующей совместных усилий образовательных учреждений, правоохранительных органов и экспертов в области информационной безопасности.

Только комплексный подход, включающий в себя технические, образовательные и психологические меры, позволит обеспечить надежную защиту будущих сотрудников от киберугроз и сохранить их морально-психологическую устойчивость в условиях современного информационного пространства.

## СПИСОК ЛИТЕРАТУРЫ

1. Кануков, А. М. О перспективах цифровизации образовательного процесса системы МВД России / А. М. Кануков, А. Х. Кодзоков // Право и управление. 2023. № 3. С. 125-129. DOI 10.24412/2224-9133-2023-3-125-129.
2. Кузнецова, Н. В. Педагогические условия формирования информационно-правовой компетенции сотрудников правоохранительных органов в центрах профессиональной подготовки диссертация на соискание ученой степени кандидата педагогических наук / Кузнецова Наталья Владимировна, 2023. 162с.
3. Грачев, М. И. Математическая модель для принятия решений по противодействию киберугрозам в производстве / М. И. Грачев, В. Г. Бурлов // Информационные технологии в проектировании и производстве. 2022. № 4(188). С. 22-27. DOI 10.52190/2073-2597\_2022\_4\_22.
4. Грачева, Н. Г. Формирование профессиональных компетенций при подготовке специалистов для органов внутренних дел // Актуальные проблемы административного и административно-процессуального права (Сорокинские чтения): Сборник статей по материалам межд. научно-практ. Конф., Санкт-Петербург, 21 марта 2025 года. СПб: СПбУ МВД РФ, 2025. С. 889-892. EDN GKYTIA.



УДК 378.147

**ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПРОВЕДЕНИИ  
ЗАНЯТИЙ В ВОЕННОЙ ОРДЕНА ЖУКОВА АКАДЕМИИ ВОЙСК  
НАЦИОНАЛЬНОЙ ГВАРДИИ РОССИЙСКОЙ ФЕДЕРАЦИИ****Григорьев Олег Вячеславович**

Академия войск национальной гвардии

Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия

e-mail: 13141208@mail.ru

**Аннотация:** Статья посвящена проблемным вопросам обеспечения информационной безопасности при проведении занятий в Военной ордена Жукова академии войск национальной гвардии Российской Федерации, таким как управление доступом к системам, использование средств криптографии и антивирусной защиты, проведение регулярного аудита и резервного копирования данных и тп.

**Ключевые слова:** информационная безопасность; меры по защите секретной информации; управление доступом к системам; использование средств криптографии; антивирусная защита.

**ISSUES OF ENSURING INFORMATION SECURITY DURING CLASSES IN THE MILITARY ORDER  
OF ZHUKOV ACADEMY OF THE NATIONAL GUARD TROOPS OF THE RUSSIAN FEDERATION****Grigoriev Oleg**

Academy of the National Guard Troops

1 Pilot Pilyutova St, St. Petersburg, 198206, Russia

e-mail: 3141208@mail.ru

**Abstract.** The article is devoted to the problematic issues of ensuring information security during classes at the Military Order of Zhukov Academy of the National Guard Troops of the Russian Federation, such as access control to systems, the use of cryptography and anti-virus protection, regular auditing and data backup, etc.

**Keywords:** information security; measures to protect classified information; system access control; use of cryptographic tools; antivirus protection.

В период проведения Специальной военной операции на Украине (далее — СВО) происходит обострение международной военно-политической обстановки. Усиление и усложнение информационного противостояния раскручивается, на фоне попыток наших «западных партнеров» манипулировать общественным сознанием в Российской Федерации. В создавшихся условиях Российскому государству нужна по-настоящему сильная правоохранительная система. Одним из органов способных корректно сдерживать, а при необходимости и жестко блокировать «информационные атаки» коллективного Запада является Федеральная служба войск национальной гвардии (далее — Росгвардия) [1].

Так, например, система обеспечения ИБ в Военной академии Росгвардии включает меры по защите секретной информации, управлению доступом к системам, использованию средств криптографии и антивирусной защиты, проведению регулярного аудита и резервного копирования данных. Учитывается специфический характер информации и требования нормативно-правовой базы, например, Доктрины информационной безопасности России, которая подчеркивает необходимость защиты данных.

Основные направления и меры обеспечения ИБ в рамках Военной академии Росгвардии:

Технические меры: использование шифрования для защиты данных на носителях и при передаче по каналам связи; блокировка нежелательных подключений и защита от внешних угроз, таких как вирусы и шпионские программы; установка и обновление антивирусного программного обеспечения для предотвращения заражения систем; контроль и предотвращение несанкционированной передачи конфиденциальной информации; создание копий данных и информационных систем для обеспечения возможности их восстановления после сбоев или аварий [2].

Организационные меры: в Военной академии Росгвардии внедрены строгие правила и процедуры для контроля доступа к информационным системам и ресурсам, ведение журналов всех действий пользователей и системных событий для анализа и выявления подозрительной активности.

Обучение персонала: проведение инструктажей и обучения военнослужащих, сотрудников и курсантов Военной академии Росгвардии основам информационной безопасности и правилам работы с конфиденциальными данными [3].

Наконец, необходимо отметить, что в Военной академии Росгвардии постоянно функционируют представители собственной безопасности, которые, при необходимости, сообщают о нарушениях ИБ в органы Федеральной службы безопасности Российской Федерации.

**СПИСОК ЛИТЕРАТУРЫ**

1. Цеханович, Д.Б., Панкратов, В.С. Каким быть современному военному образованию / Армейский сборник. 2022. № 12. Электронный ресурс: <http://army.ric.mil.ru/Stati/item/456129/> (дата обращения: 09.09.2025).
2. Рузов А., Князьков А. Информационная безопасность курсантов военных институтов // Сб. учеб.-метод. мат.-лов «Войсковой вестник». Прил. к журн. «На боевом посту». 2024. № 2. С. 57-61.
3. В Москве откроют центр кибербезопасности Росгвардии. Электронный ресурс: <https://www.vedomosti.ru/society/news/2021/04/27/867838-moskve-otkroyut-tsentr-kiberbezopasnosti-rosgvardii> (дата обращения: 09.09.2025).

УДК 37.018.43:004

**ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРЕПОДАВАНИИ ДИСЦИПЛИН  
ГУМАНИТАРНОГО ПРОФИЛЯ: ВЫЗОВЫ И ПЕРСПЕКТИВЫ****Евстратова Юлиана Айратовна**

Академия войск национальной гвардии

Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия

e-mail: yuliana130682@mail.ru

**Аннотация.** Статья посвящена анализу современных тенденций применения информационных технологий (ИТ) в образовательном процессе по дисциплинам гуманитарного профиля. В условиях цифровой трансформации общества традиционные методики преподавания истории, филологии, культурологии и философии требуют значительной модернизации.

**Ключевые слова:** информационные технологии; гуманитарное образование; цифровизация; Digital Humanities; виртуальная реальность; LMS; дистанционное обучение; педагогические методы.

**THE APPLICATION OF INFORMATION TECHNOLOGY IN TEACHING HUMANITIES  
DISCIPLINES: CHALLENGES AND PROSPECTS****Evstratova Yuliana**

Academy of the National Guard Troops

1 Pilot Pilyutova St, St. Petersburg, 198206, Russia

e-mail: yuliana130682@mail.ru

**Abstract.** The article is devoted to the analysis of modern trends in the use of information technologies (IT) in the educational process in the disciplines of the humanities. In the context of the digital transformation of society, traditional methods of teaching history, philology, cultural studies and philosophy require significant modernization.

**Keywords:** information technology; humanitarian education; digitalization; Digital Humanities; virtual reality; LMS; distance learning; pedagogical methods.

Современный этап развития общества характеризуется глубокой интеграцией информационных технологий во все сферы жизни, включая образование. Если в преподавании точных и естественных наук использование ИТ стало давно устоявшейся нормой, то в гуманитарных дисциплинах этот процесс носит более сложный и зачастую дискуссионный характер [1]. Гуманитарное знание, традиционно основанное на работе с текстами, интерпретации, критическом анализе и живом диалоге, сталкивается с необходимостью адаптации к цифровой среде. Актуальность данного исследования обусловлена потребностью в систематизации существующих практик, выявлении эффективных моделей и предупреждении возможных рисков, связанных с цифровизацией гуманитарного образования.

Применение ИТ в гуманитарном образовании можно условно разделить на несколько уровней. Базовый уровень. Использование мультимедийного контента (аудио-, видеофрагменты, интерактивные карты, презентации) для повышения наглядности и эмоционального воздействия. Например, использование интерактивных карт в исторических дисциплинах (Google Earth, Histography) позволяет визуализировать военные кампании или изменения государственных границ [2].

Организационный уровень. Применение систем управления обучением (LMS), таких как Moodle, Canvas, Blackboard. Эти платформы организуют учебный процесс, предоставляя возможности для размещения материалов, проведения тестирований, организации форумов и контроля успеваемости [3].

Интерактивный уровень. Внедрение вебинаров, видеоконференций, онлайн-курсов (МООС) и интерактивных заданий. Это позволяет реализовать дистанционное и смешанное обучение, обеспечивая обратную связь и коллаборацию между студентами.

Применение информационных технологий в преподавании гуманитарных дисциплин является необратимым и необходимым процессом, отвечающим вызовам времени. Оно открывает беспрецедентные возможности для визуализации, анализа и доступа к информации, трансформируя традиционную классно-урочную систему в более гибкую и персонализированную.

Однако ключевым выводом является то, что технология сама по себе не гарантирует повышения качества образования. Эффективность ее применения целиком зависит от педагогического дизайна, методической грамотности преподавателя и его способности органично встроить цифровые инструменты в образовательный процесс. Перспективы дальнейших исследований видятся в разработке конкретных методик для различных гуманитарных дисциплин, оценке долгосрочного влияния цифровых форматов на глубину усвоения материала и подготовке нового поколения педагогов-гуманитариев, синтезирующих традиционную академическую культуру с современными цифровыми компетенциями.

**СПИСОК ЛИТЕРАТУРЫ**

1. Роберт И.В. Теория и методика информатизации образования (психолого-педагогич. и технологич. аспекты). М.: ИИО РАО, 2010. 274 с.
2. Bodenhamer, D. J., Corrigan, J., & Harris, T. M. (Eds.). The Spatial Humanities: GIS and the Future of Humanities Scholarship. Indiana University Press, 2015.
3. Патаракин Е.Д. Сетевые сообщества и обучение. М.: НИИ школьных технологий, 2010. 176 с.

УДК 004.94:512.643

**ЭФФЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННЫХ УЧЕБНО-ТРЕНИРОВОЧНЫХ СРЕДСТВ  
В ПРОЦЕССЕ ОБУЧЕНИЯ КУРСАНТОВ ИНЖЕНЕРНО-ТЕХНИЧЕСКОГО ПРОФИЛЯ****Егоренков Сергей Александрович**

Академия войск национальной гвардии

Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия

e-mail: egorenkoff83@mail.ru

**Аннотация.** Представлен опыт применения учебно-тренировочных средств в процессе обучения курсантов дисциплинам инженерно-технического профиля. Использование электронных тренажеров способствует закреплению умений и навыков у обучающихся в ходе подготовки по специальности. Произведен сравнительный анализ результатов обучения курсантов, использующих учебно-тренировочные средства, с результатами обучения без их применения.

**Ключевые слова:** учебно-тренировочное средство; инженерно-технический профиль; сравнительный анализ; программное обеспечение; полигон.

**THE EFFECTIVENESS OF USING ELECTRONIC EDUCATIONAL AND TRAINING TOOLS  
IN THE PROCESS OF TRAINING CADETS OF AN ENGINEERING PROFILE****Egorenkov Sergey**

Academy of the National Guard Troops

1 Pilot Pilyutova St, St. Petersburg, 198206, Russia

e-mail: egorenkoff83@mail.ru

**Abstract.** The experience of using educational and training tools in the process of teaching cadets disciplines of engineering and technical profile is presented. The use of electronic simulators helps to consolidate the skills of students during their training in the specialty. A comparative analysis of the results of the training of cadets using educational and training tools with the results of training without their use has been carried out.

**Keywords:** educational and training equipment; engineering and technical profile; comparative analysis; software; polygon.

Сложившиеся военно-политические условия в мире и стране продиктовали потребность в инженерно-технической подготовке курсантов, как будущих офицеров-артиллеристов Росгвардии. На кафедре боевого применения артиллерийских подразделений факультета (командно-артиллерийского) Военной ордена Жукова академии войск национальной гвардии Российской Федерации осуществляется подготовка обучающихся по дисциплинам инженерно-технического профиля по специальности. Совершенствование системы подготовки курсантов во многом связано с разработкой и внедрением новых учебно-тренировочных средств.

Учебно-тренировочные средства формируют практические навыки, позволяющие отрабатывать действия до автоматизма с визуализацией сложных процессов, в тоже время создаются безопасные условия для отработки действий.

В ходе обучения курсантов используются электронные учебно-тренировочные средства, позволяющие обучать стрельбе из противотанковых ракетных комплексов, стрельбе артиллерии из закрытых огневых позиций, проведение расчетов топографических данных по цели, поправки на метеорологические и баллистические условия стрельбы, а также управлению БПЛА различных типов. Формирование кадрового потенциала в этой высокотехнологичной сфере начинается уже на уровне школьного образования, где особый акцент делается на развитии критически важных для операторов навыков пространственного мышления и топографической привязки [1].

Особое место занимает компьютерный артиллерийский полигон «Артерра-ВТ-3Д», предназначенный для обучения специалистов стрельбе и управлению огнем артиллерийских подразделений в звене: дивизион- батарея- взвод-орудие. Обучающиеся выполняют огневые задачи в различных погодных условиях и в любое время суток. Упрощенная версия тренажера «Артерра» установлена на компьютеры обучающихся и позволяет самостоятельно вырабатывать навыки по стрельбе и управлению огнем артиллерийских подразделений [2, 3].

Применения учебно-технических средств для обучения, это неотъемлемый элемент компетентного подхода в образовании, позволяющий подготовить специалиста высокого уровня. Применение тренажеров позволяет экономить время, финансовые ресурсы, в тоже время создать доступную систему обучения.

**СПИСОК ЛИТЕРАТУРЫ**

1. Принцев Н. В., Егоренков С. А. Педагогические аспекты тактики применения боевых дронов и особенности компоновочных схем. Педагогический журнал. 2025. Т. 15. № 2-1. С. 189-197.
2. Теремков Е. М., Буфетов Н. Н., Репин А. В. Формирование профессиональных качеств военных специалистов посредством применения электронного обучения и дистанционных образовательных технологий. Военная мысль. 2020. № 11. С. 146-153.
3. Базунов С.С., Гольке Д.Е. Технологии дистанционного обучения. Перспективные подходы в обучении курсантов // Актуальные исследования. 2021. № 23(50). С. 36-39

УДК 004.94:512.643

**ЭФФЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ АДДИТИВНЫХ ТЕХНОЛОГИЙ В ПРОЦЕССЕ ОБУЧЕНИЯ КУРСАНТОВ ИНЖЕНЕРНО-ТЕХНИЧЕСКОГО ПРОФИЛЯ****Егоренков Сергей Александрович, Егоренкова Юлия Викторовна**

Академия войск национальной гвардии

Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия

e-mails: egorenkoff83@mail.ru, egorenkovaylia@mail.ru

**Аннотация.** Представлен опыт применения программ Компас 3D, Blender, 3D Builder, Repiter Host, Ultimaker Cura. Данные программы позволяют обучающимся эффективно разработать, создать трёхмерную компьютерную графику, 3D объекты, подготовить их к 3D печати.

**Ключевые слова:** Компас 3D; Blender; 3D Builder; Repiter Host; Ultimaker Cura; 3D печать.

**EFFECTIVENESS OF USING ADDITIVE TECHNOLOGIES IN THE PROCESS OF TEACHING ENGINEERING STUDENTS****Egorenkov Sergey, Egorenkova Julia**

Academy of the National Guard Troops

1 Pilot Pilyutova St, St. Petersburg, 198206, Russia

e-mails: egorenkoff83@mail.ru, egorenkovaylia@mail.ru

**Abstract.** The experience of using the programs Compass 3D, Blender, 3D Builder, Repiter Host, Ultimaker Cura. These programs allow students to effectively develop, create three-dimensional computer graphics, 3D objects, prepare them for 3D printing.

**Keywords:** Kompas 3D; Blender; 3D Builder; Repiter Host; Ultimaker Cura; 3D read.

Подготовка курсантов инженерно-технического профиля осуществляется с 2024 года на базе Военной ордена Жукова академии войск национальной гвардии Российской Федерации.

В настоящее время идет развитие материально-технической базы, одним из приоритетным направлений является обучение работе в инженерных программах с применением аддитивных технологий, основанных на создании физического объекта по электронной геометрической модели путем добавления материала, как правило, слой за слоем, в отличие от вычитающего (субтрактивного) производства (механической обработки) и традиционного формообразующего производства (литья, штамповки) [1].

В настоящее время курсантами осваиваются программы Компас 3D, Blender, 3D Builder, Repiter Host, Ultimaker Cura. В рамках военно-научного общества курсанты учатся 3D печати.

В наше время технологии 3D моделирования наиболее значимы, чем когда-либо. Применение 3D-технологий имеет место во многих сферах жизни человека находит свое отражение в разнообразных областях науки, техники и индустрии развлечений [2].

Термины «аддитивные технологии» и «3D-печать» часто используют как синонимы. Термин «3D-печать» появился раньше и его чаще употребляют, когда речь идет о недорогих домашних принтерах. В масштабах промышленного производства обычно говорят об аддитивных технологиях [3].

Появление среды по 3D-моделированию дало огромный скачок в развитии инженерии, а также других отраслей науки [4]. Внедрение 3D-печати в процесс обучения курсантов — это стратегическое вложение в подготовку высококвалифицированных, мыслящих и адаптивных специалистов для всех видов силовых структур.

В ходе обучения происходит практическое закрепление теории, курсанты наблюдают, как происходит превращение абстрактных чертежей и схем в осязаемые модели, также происходит развитие инженерного и конструкторского мышления, глубокое понимание принципов работы, сборки и взаимосвязи деталей. Развиваются навыки по созданию прототипов и оперативного решения инженерных задач. Создаются библиотеки 3D-моделей учебной материальной базы и учебных образцов вооружения.

Внедрение 3D-печати — это эволюционный шаг в военном образовании. Оно развивает не только технические навыки, но и критическое мышление, инициативу и способность к креативному мышлению. Курсант, научившийся проектировать и печатать недостающую деталь, становится не просто пользователем техники, а ее полноценным эксплуататором, способным поддерживать боеготовность в различных условиях.

**СПИСОК ЛИТЕРАТУРЫ**

1. ГОСТ Р 57558-2017 Национальный стандарт Российской Федерации Аддитивные технологические процессы. Базовые принципы. Ч. 1. Термины и определения.
2. Сергеева В.С., Бысова Т.В., Смирнов В.А., Поначугин А.В. Проблемы применения методов 3D-моделирования и 3D-печати в науке и производстве. Нижегородский Государственный педагогический университет имени Козьмы Минина, Нижний Новгород, 2021, 32 с.
3. Федоров Р.Ю., Шмидт А.Д., Глушков К.А. СЕКЦИЯ X. МОДЕЛИРОВАНИЕ Перспективные направления использования аддитивных технологий для обучения курсантов военных вузов Пермский военный институт войск национальной гвардии. Пермь, 2023. 88 с.
4. Корчинов И.Д., Абросимов А.В., Васильев Ф.А. Создание трёхмерных моделей в программной среде КОМПАС-3D для последующей 3D-печати. Иркутский государственный аграрный университет им. А.А. Ежевского, Молодежный, Иркутский р-н, Иркутская обл., 2024. 115 с.

УДК 340.01

**ПОВЫШЕНИЕ ЛИЧНОЙ БЕЗОПАСНОСТИ ВОЕННОСЛУЖАЩИХ ПОСРЕДСТВОМ  
ОРГАНИЗАЦИИ ПРОТИВОДЕЙСТВИЯ ДЕЗИНФОРМАЦИИ****Калкаманов Эмиль Ильясович, Донцов Иван Алексеевич**

Академия войск национальной гвардии

Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия

e-mail: emil.rosgvardia@mail.ru, doncovivan@bk.ru

**Аннотация.** В условиях современного информационного общества противодействие дезинформации становится одной из ключевых задач для обеспечения стабильности и безопасности. Дезинформация, представляющая собой преднамеренное распространение ложной или искаженной информации, может иметь серьезные последствия для общественного мнения, политической ситуации и социальных процессов. В заключение подчеркивается важность совместных усилий общества, медиаплатформ и образовательных учреждений в создании устойчивой информационной среды, способной противостоять угрозам дезинформации.

**Ключевые слова:** информационная безопасность; дезинформация; личная безопасность; учебные программы; алгоритмы.

**APPLICATION OF GAME THEORY ALGORITHMS AND PROCEDURES TO ENSURING  
INFORMATION SECURITY IN STRUCTURAL UNITS  
OF LAW ENFORCEMENT AGENCIES****Kalkamanov Emil, Doncov Ivan**

Academy of the National Guard Troops

Pilot Pilyutova St, 1, St. Petersburg, 198206, Russia

e-mail: emil.rosgvardia@mail.ru, 89513325199@mail.ru

**Abstract.** In the context of the modern information society, countering disinformation is becoming one of the most important tasks for ensuring stability and security. Misinformation, which is the deliberate dissemination of false or distorted information, can have serious consequences for public opinion, the political situation and social processes. In conclusion, the importance of joint efforts of bestoru and educational institutions in creating a stable information environment capable of.

**Keywords:** information security; disinformation; personal security; training programs; algorithms.

Противодействие дезинформации требует комплексного подхода, включающего развитие медийной грамотности среди населения, внедрение эффективных механизмов проверки фактов и сотрудничество между государственными институтами, частным сектором и гражданским обществом для создания устойчивой информационной среды, способствующей критическому мышлению и осознанному восприятию информации [4].

В современном мире, где информация распространяется с беспрецедентной скоростью, дезинформация становится одной из главных угроз для демократических процессов, общественного здоровья и социальной стабильности. С учетом этих вызовов необходимо разработать стратегии, направленные на минимизацию негативного влияния ложной информации [1].

Первым шагом в борьбе с дезинформацией является повышение уровня медийной грамотности среди населения. Это включает в себя [2]:

1. Внедрение курсов по медийной грамотности в образовательные учреждения, начиная с начальной школы и заканчивая вузами. Учебные программы должны обучать курсантов, различать надежные источники информации от ненадежных, а также развивать навыки критического анализа информации.

2. Поддержка независимых организаций, занимающихся проверкой фактов, которые могут оперативно реагировать на распространение дезинформации и предоставлять достоверные данные [3].

3. Разработка алгоритмов и инструментов на основе искусственного интеллекта для автоматического выявления и маркировки подозрительной информации в социальных сетях и на новостных платформах.

Для эффективного противодействия дезинформации необходимо сотрудничество между различными секторами общества:

1. Государственные органы должны создавать законодательные инициативы, направленные на борьбу с дезинформацией, обеспечивая при этом защиту свободы слова.

2. Платформы социальных медиа должны принимать активное участие в борьбе с дезинформацией, внедряя прозрачные алгоритмы модерации контента и предоставляя пользователям инструменты для отчетности о ложной информации [4].

3. Неправительственные организации и активисты играют ключевую роль в просвещении населения о рисках дезинформации и в организации кампаний по повышению осведомленности.

**СПИСОК ЛИТЕРАТУРЫ**

1. Авдеенко И. А., Шунейко А. С. «Информационная безопасность человека» (2018) // URL: <https://www.litres.ru/book/aleksan> (дата обращения: 25.08.2025).
2. Каширина Е. И., Никляева А. С. «Дезинформация: анализ, последствия и противодействие» (2024) // URL: [https://www.elibrary.ru/start\\_sess](https://www.elibrary.ru/start_sess) (дата обращения: 25.08.2025).
3. Михеев Е. А., Нестик Т. А. «Дезинформация в социальных сетях: состояние и перспективы психологических исследований» (2018).

Статья опубликована в журнале «Социальная психология и общество», том 9, номер 2, страницы 5–20 // URL: <https://psyjournals.ru/journals/sps/archive> (дата обращения: 25.08.2025).

4. Федеральный закон от 08.08.2024 N 216-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации» // URL: <https://www.consultant.ru/document> (дата обращения: 25.08.2025).

УДК 004.056.5

## ИСТОРИЧЕСКИЕ АСПЕКТЫ ВОЗНИКНОВЕНИЯ И РАЗВИТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Орехов Александр Валерьевич, Гежа Марат Анатольевич**

Академия войск национальной гвардии

Летчика Пилотова ул., 1, Санкт-Петербург, 198206, Россия

e-mails: orexow28@mail.ru, gejaaMA@mail.ru

**Аннотация.** В данной статье рассматриваются этапы развития средств информационных коммуникаций. Решение определенных задач информационной безопасности, на каждом этапе.

**Ключевые слова:** информационная безопасность; средства информационных коммуникаций; этапы развития; угроза информационной безопасности; получение информации.

## HISTORICAL ASPECTS OF THE EMERGENCE AND DEVELOPMENT OF INFORMATION SECURITY

**Orechov Aleksandr, Gezha Marat**

Academy of the National Guard Troops

1 Pilot Pilyutova St, St. Petersburg, 198206, Russia

e-mails: orexow28@mail.ru, gejaaMA@mail.ru

**Abstract.** This article discusses the stages of development of information communication tools. The solution of certain information security tasks at each stage.

**Keywords:** information security; means of information communications; stages of development; information security threat; obtaining information.

Информационная безопасность возникла с появлением средств информационных коммуникаций между людьми, а также с осознанием человека о наличии сообществ интересов, которым может быть нанесен ущерб путём воздействия на них. Средства информационных коммуникаций обусловили наличие и развитие средств, которые обеспечили информационный обмен между всеми элементами социума. Учитывая влияние на трансформацию идей информационной безопасности, в развитии средств информационных коммуникаций можно выделить несколько этапов [1].

Первый этап — до 1816 года. Характеризуется использованием естественно возникавших средств информационных коммуникаций. В этот период основная задача информационной безопасности заключалась в защите сведений о событиях, фактах, имуществе, местонахождении и других данных, имеющих для человека лично или сообщества, к которому он принадлежал, жизненное значение.

Второй этап, начиная с 1816 года, связан с началом использования искусственно создаваемых технических средств и радиосвязи. Для обеспечения скрытности и помехозащищенности радиосвязи необходимо было использовать опыт первого периода информационной безопасности на более высоком технологическом уровне, а именно применение помехоустойчивого кодирования сообщения (сигнала) с последующим декодированием принятого сообщения (сигнала).

Третий этап — начиная с 1935 года, связан с появлением радиолокационных и гидроакустических средств. Основным способом обеспечения информационной безопасности в этот период было сочетание организационных и технических мер, направленных на повышение защищенности радиолокационных средств от воздействия на их приемные устройства активными маскирующими и пассивными имитирующими радиоэлектронными помехами.

Четвертый этап — начиная с 1946 года, связан с изобретением и внедрением в практическую деятельность электронно-вычислительных машин (компьютеров). Задачи информационной безопасности решались, в основном, методами и способами ограничения физического доступа к оборудованию средств добывания, переработки и передачи информации.

Пятый этап — начиная с 1965 года, обусловлен созданием и развитием локальных информационно-коммуникационных сетей. Задачи информационной безопасности также решались, в основном, методами и способами физической защиты средств добывания, переработки и передачи информации, объединённых в локальную сеть путём администрирования и управления доступом к сетевым ресурсам.

Шестой этап — начиная с 1973 года — связан с использованием сверхмобильных коммуникационных устройств с широким спектром задач. Угрозы информационной безопасности стали гораздо серьезнее. Для обеспечения информационной безопасности в компьютерных системах с беспроводными сетями передачи данных потребовалась разработка новых критериев безопасности. Образовались сообщества людей — хакеров, ставящих своей целью нанесение ущерба информационной безопасности отдельных пользователей, организаций

и целых стран. Информационный ресурс стал важнейшим ресурсом государства, а обеспечение его безопасности — важнейшей и обязательной составляющей национальной безопасности. Формируется информационное право — новая отрасль международной правовой системы.

Седьмой этап, начиная с 1985 года, связан с созданием и развитием глобальных информационно-коммуникационных сетей, с использованием космических средств обеспечения. Можно предположить, что очередной этап развития информационной безопасности, очевидно, будет связан с широким использованием мобильных коммуникационных устройств с широким спектром задач и глобальным охватом в пространстве и времени, обеспечиваемым космическими информационно-коммуникационными системами. Для решения задач информационной безопасности, на этом этапе необходимо создание макросистемы информационной безопасности человечества под эгидой ведущих международных форумов [2–4].

Таким образом, в современном мире уже существует множество способов передачи и получения информации — компьютер (интернет), средства связи (электронная почта, мобильные телефоны), индустрия (цифровое телевидение), транспорт (аэронавигация), торговля (интернет-магазины, кредитные карты), медицина (оборудование, медицинские архивы), и т.д. Информационная безопасность состоит в защите этой информации методами предотвращения, обнаружения и немедленного реагирования, а также постоянного совершенствования средств защиты информации.

#### СПИСОК ЛИТЕРАТУРЫ

1. Безопасность: теория, парадигма, концепция, культура. Словарь-справочник / В. Ф. Пилипенко. 2-е изд., доп. и перераб. М.: ПЕР СЭ-Пресс, 2008.
2. Информационная безопасность (2-я кн. соц.-полит. проекта «Актуальные проблемы безопасности социума»). М.: «Оружие и технологии», 2009.
3. Домарев В. В. Безопасность информационных технологий. Системный подход К.: ООО ТИД Диа Софт, 2004.
4. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий» (ГОСТ Р ИСО/МЭК 13335-1-2012).

УДК 004.056.5

#### ОСНОВНЫЕ СОСТАВЛЯЮЩИЕ, ПОСТРОЕНИЕ И ЭКСПЛУАТАЦИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Орехов Александр Валерьевич, Карсаков Никита Романович**

Академия войск национальной гвардии

Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия

e-mails: orexow28@mail.ru, charsakov@mail.ru

**Аннотация.** В данной статье рассматриваются основные составляющие информационной безопасности, построение и эксплуатация системы обеспечения информационной безопасности.

**Ключевые слова:** система обеспечения информационной безопасности; доступность информации; целостность информации; конфиденциальность информации; защита информации.

#### THE MAIN COMPONENTS, CONSTRUCTION, AND OPERATION OF AN INFORMATION SECURITY SYSTEM

**Orekhov Aleksandr, Karsakov Nikita**

Academy of the National Guard Troops

1 Pilot Pilyutova St, St. Petersburg, 198206, Russia

e-mails: orexow28@mail.ru, charsakov@mail.ru

**Abstract.** This article discusses the main components of information security, as well as the construction and operation of an information security system.

**Keywords:** information security system; information availability; information integrity; and information confidentiality; information protection.

Под информационной безопасностью понимается — защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Спектр интересов субъектов, связанных с использованием информационных систем, можно разделить на следующие составляющие: обеспечение доступности, целостности и конфиденциальности информационных ресурсов и поддерживающей инфраструктуры [1].

Иногда в число основных составляющих информационной безопасности включают защиту от несанкционированного доступа к информации, под которым понимают доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств. В то же время обеспечение конфиденциальности как раз и подразумевает защиту от несанкционированного доступа.

Трактовка проблем, связанных с информационной безопасностью, для разных категорий субъектов может существенно различаться. Для иллюстрации достаточно сопоставить режимные государственные организации и

учебные заведения. В первом случае «пусть лучше все сломается, чем враг узнает хотя бы один секрет», во втором — «да лет у нас никаких секретов, лишь бы все работало».

Информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации, это принципиально более широкое понятие. Субъект информационных отношений может пострадать не только от несанкционированного доступа, но и от поломки системы, вызвавшей перерыв в работе [2].

Доступность информации — свойство системы обеспечивать своевременный беспрепятственный доступ правомочных (авторизованных) субъектов к интересующей их информации или осуществлять своевременный информационный обмен между ними. Информационные системы создаются для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, это, очевидно, наносит ущерб всем субъектам информационных отношений. Особенно ярко ведущая роль доступности проявляется в разного рода системах управления — производством, транспортом и т.п. Внешне менее драматичные, но также весьма неприятные последствия — и материальные, и моральные — может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей [3].

Целостность информации — свойство информации, характеризующее ее устойчивость к случайному или преднамеренному разрушению, или несанкционированному изменению. Целостность можно подразделить на статическую и динамическую. Средства контроля динамической целостности применяются, в частности, при анализе потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений. Целостность оказывается важнейшим аспектом информационной безопасности в тех случаях, когда информация служит руководством к действию. Рецептура лекарств, предписанные медицинские процедуры, набор и характеристики комплектующих изделий, ход технологического процесса — все это примеры информации, нарушение целостности которой может оказаться в буквальном смысле смертельным.

Конфиденциальность информации — свойство информации быть известной и доступной только правомочным субъектам системы (пользователям, программам, процессам). Конфиденциальность — самый проработанный у нас в стране аспект информационной безопасности. К сожалению, практическая реализация мер по обеспечению конфиденциальности современных информационных систем наталкивается в России на серьезные трудности. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные препоны и технические проблемы.

Если вернуться к анализу интересов различных категорий субъектов информационных отношений, то почти для всех, кто реально использует ИС, на первом месте стоит доступность. Практически не уступает ей по важности целостность — какой смысл в информационной услуге, если она содержит искаженные сведения. Наконец, конфиденциальная информация есть как у организаций, так и отдельных пользователей.

Таким образом целью реализации информационной безопасности какого-либо объекта является построение системы обеспечения информационной безопасности данного объекта. Для построения и эффективной эксплуатации системы обеспечения информационной безопасности необходимо: выявить требования защиты информации, специфические для данного объекта защиты; учесть требования национального и международного Законодательства; использовать наработанные практики построения подобных системы обеспечения информационной безопасности; определить подразделения, ответственные за реализацию и поддержку системы обеспечения информационной безопасности; распределить между подразделениями области ответственности в осуществлении требований системы обеспечения информационной безопасности. В дальнейшем система обеспечения информационной безопасности, корректируется для эффективного выполнения своих задач защиты информации и соответствия новым требованиям постоянно обновляющейся информационной системы.

#### СПИСОК ЛИТЕРАТУРЫ

1. Безопасность: теория, парадигма, концепция, культура. Словарь-справочник / В. Ф. Пилипенко. 2 е изд., доп. и перераб. М.: ПЕР СЭ-Пресс, 2008.
2. Малюк А. А., Полянская О. Ю. Комментарии к Доктрине информационной безопасности РФ. М.: Горячая линия Телеком, 2018.
3. Национальный стандарт РФ «Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий» (ГОСТ Р ИСО/МЭК 13335-1-2012).

УДК 004.94:512.643

#### **ПРИМЕНЕНИЕ АЛГОРИТМОВ И ПРОЦЕДУР ТЕОРИИ ИГР ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СТРУКТУРНЫХ ПОДРАЗДЕЛЕНИЯХ СИЛОВЫХ ВЕДОМСТВ**

**Примакин Алексей Иванович, Таратухин Никита Алексеевич**

Академия войск национальной гвардии

Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия

e-mails: a.primakin@mail.ru, nik.taratuxin@mail.ru

**Аннотация.** Рассматривается вопрос о применении теории игр для обеспечения информационной безопасности в структурных подразделениях силовых ведомств, в частности, для выбора средства эффективной



защиты объектов информатизации от различного рода кибератак. Для выбора и формирования оптимального набора средств защиты объекта информатизации предлагается применение алгоритмов теории игр, платежные матрицы которых сводятся к моделированию конфликтных ситуаций и выбору оптимальных стратегий.

**Ключевые слова:** информационная безопасность; математические методы; теория игр; оптимальный набор; объект информатизации.

## APPLICATION OF GAME THEORY ALGORITHMS AND PROCEDURES TO ENSURING INFORMATION SECURITY IN STRUCTURAL UNITS OF LAW ENFORCEMENT AGENCIES

Primakin Aleksey, Taratukhin Nikita

Academy of the National Guard Troops

1 Pilot Pilyutova St, St. Petersburg, 198206, Russia

e-mails: a.primakin@mail.ru, nik.taratuxin@mail.ru

**Abstract.** The article considers the issue of the application of game theory to ensure information security in the structural divisions of law enforcement agencies, in particular, to choose a means of effective protection of informatization objects from various kinds of cyber attacks. To select and form the optimal set of means of protecting the object of informatization, the application of game theory algorithms is proposed, the payment matrices of which are reduced to modeling conflict situations and choosing optimal strategies based on the criteria.

**Keywords:** information security; mathematical methods; game theory; optimal set; informatization object.

Актуальность темы определяется необходимостью решения задач по обеспечению информационной безопасности, что в значительной степени продиктовано сложившимися военно-политическими условиями в стране и мире [1]. Решение этих задач связано с обеспечением конфиденциальности, доступности и целостности информационных потоков, что обеспечивается благодаря правовым, организационно-техническим и экономическим методам защиты информации [2].

Интересующая нас область организационных методов защиты, в первую очередь, связана с определением направлений и методик разработки политики безопасности структурных подразделений силовых ведомств.

Для решения ряда частных задач в этой области необходим соответствующий математический инструментарий. Задачи, требующие оперативного и рационального принятия решений, могут быть лучше решены с помощью теории игр [3, 4].

Теория игр, как раздел прикладной математики, сводится к моделированию ситуации, в которой противостоящие друг другу стороны (обычно их называют игроками) принимают связанные и зависимые друг от друга решения, называемые стратегиями.

В этой ситуации каждый игрок, вырабатывая и принимая ту или иную стратегию, учитывает возможные стратегии, принимаемые другим игроком.

Для поиска оптимального набора средств защиты объектов информатизации структурного подразделения силового ведомства от различного рода кибератак можно предложить двухстороннюю математическую игру, в которой одним из игроков выступает сама система защиты объекта информатизации, а в качестве игрока-противника — возможные атаки нарушителя-хакера.

Поскольку цель — это определение оптимальной стратегии, принимаемой администратором сети, при которой возможные потери от нападения на объект информатизации нарушителем-хакером будут минимальны, будем считать, что цель противника в этой ситуации — нанести как можно больший ущерб атакуемому объекту.

Эту ситуацию можно определить формулой: возможный «выигрыш» хакера равносителен «проигрышу» администратора сети.

Часто возникают ситуации, когда один из игроков, допустим «защитник» объекта информатизации, имеет не полную информацию о действиях противника, может только предполагать о принимаемых нарушителем-хакером решениях и стратегиях.

В этом случае для практического применения теории игр необходим набор конечных и предсказуемых хакерских стратегий, построенных на вероятностных моделях, сформированных на результатах анализа статистических данных за предшествующий период времени.

## СПИСОК ЛИТЕРАТУРЫ

1. Директива Росгвардии от 28 октября 2021 г. № Д-2 «О приоритетных направлениях деятельности войск национальной гвардии Российской Федерации в 2022 году» // Сайт Росгвардии. URL: <https://rosguard.gov.ru/> (дата обращения: 20.07.2025).
2. Доктрина информационной безопасности Российской Федерации // URL: <https://rg.ru/documents/2016/12/06/doktrina-infobezobasnost-site-dok.html> (дата обращения: 20.07.2025).
3. Басараб М. А. Теория игр в информационной безопасности: учебно-методическое пособие / М. А. Басараб, Н. С. Коннова. Москва: МГТУ им. Н.Э. Баумана, 2019. 80 с. // URL: <https://ibooks.ru/bookshelf/374903/reading> (дата обращения: 20.07.2025).
4. Викснин И. И., Мариненков Е. Д., Чупров С. С. Применение теории игр для обеспечения безопасности коммуникации киберфизической системы с использованием механизмов репутации и доверия // Научно-технический вестник информационных технологий, механики и оптики. 2022. Т. 22, № 1. С. 47-59.

УДК 004.056

**ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТРАНСПОРТНЫХ СИСТЕМ****Романов Демьян Александрович**

Академия войск национальной гвардии

Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия

e-mail: demyan.rom06@gmail.com

**Аннотация.** В данной работе обосновывается тезис о том, что информационная безопасность является критически важным элементом устойчивого развития современных транспортных систем. Автор утверждает, что цифровизация транспорта, повышая эффективность, создает новые уязвимости. Предлагается многоуровневая стратегия защиты, основанная на принципах проактивности и непрерывного мониторинга, без которой невозможно дальнейшее внедрение автономных технологий.

**Ключевые слова:** информационная безопасность; транспорт; защита; профилактика; шифрование данных.

**INFORMATION SECURITY OF TRANSPORT SYSTEMS****Romanov Demyan**

Academy of the National Guard Troops

1 Pilot Pilyutova St, St. Petersburg, 198206, Russia

e-mail: demyan.rom06@gmail.com

**Abstract.** This paper substantiates the thesis that information security is a critically important element for the sustainable development of modern transport systems. The author argues that the digitalization of transport, while increasing efficiency, creates new vulnerabilities. A multi-level protection strategy based on the principles of proactivity and continuous monitoring is proposed, without which the further implementation of autonomous technologies is impossible.

**Keywords:** information security; transport; protection; prevention; data encryption.

Транспортная система — это единый цифровой контур. Нельзя обеспечить безопасность по отдельности: необходимо рассматривать взаимосвязь всех компонентов — от датчиков на дороге и бортового оборудования транспортных средств (V2X — vehicle-to-everything) до центров управления и облачных платформ. Атака на один, даже периферийный, элемент может привести к каскадному отказу всей системы.

Современные киберугрозы для транспортной системы отличаются комплексным и целевым характером. К числу ключевых вызовов относятся кибератаки на объекты инфраструктуры, такие как светофоры и системы управления движением, способные парализовать жизнь мегаполиса. Серьезную опасность представляет взлом беспилотного и подключенного транспорта, когда удаленный захват управления создает прямую угрозу жизни людей.

Отдельную проблему составляют атаки на цепочки поставок, использующие уязвимости в оборудовании или программном обеспечении, которые могли быть заложены еще на этапе производства. Наконец, широко распространены кража и манипуляция данными, например, с помощью GPS-спуфинга или перехвата информации о местоположении грузов [1-3].

Для противодействия этим угрозам необходима эффективная многоуровневая стратегия безопасности, основанная на принципах «Security by Design» (безопасность на этапе проектирования) и «Zero Trust» (недоверие по умолчанию). Ее ключевыми элементами являются проактивность, то есть внедрение защитных мер уже на стадии создания систем, а не после инцидента. Не менее важен непрерывный мониторинг и обнаружение аномалий с использованием SOC-центров и SIEM-систем для анализа событий безопасности в реальном времени. Обязательной мерой выступает криптографическая защита данных, подразумевающая их шифрование как при передаче, так и при хранении. Стратегия должна включать регулярные аудиты и пентесты для активного поиска уязвимостей, а также развитие нормативно-правовой базы и стандартов, опирающихся на отечественные ГОСТы и международный опыт, такие как ISO/SAE 21434 для автомобильной кибербезопасности [4-5].

Таким образом Информационная безопасность перестала быть вспомогательной функцией и стала неотъемлемым атрибутом и обязательным условием надежного функционирования любой современной транспортной системы. Инвестиции в кибербезопасность транспорта — это инвестиции в национальную безопасность, защиту человеческих жизней и экономическую стабильность. Будущее развитие транспорта, особенно в контексте автономности, невозможно без создания устойчивой к кибератакам экосистемы.

**СПИСОК ЛИТЕРАТУРЫ**

1. ГОСТ Р 59639-2021(ISO/SAE 21434:2021). Дорожные транспортные средства. Кибербезопасность. М. Стандартинформ, 2021. 62 с.
2. ГОСТ Р МЭК 62443-1-1-2021. Сети и системы промышленной автоматизации. Информационная безопасность. Часть 1-1. Термины, понятия и модели. М.: Стандартинформ, 2021.
3. ISO/SAE 21434:2021. «Road vehicles Cybersecurity engineering». 2021.
4. NIST Special Publication 800-82 Rev. 2. «Guide to Industrial Control Systems (ICS) Security». 2015. Зегжда Д.П., Иванов М.А. Основы кибербезопасности киберфизических систем. М.: Горячая линия Телеком, 2020. 280 с.
5. Петренко С.А., Курбанов Б.К. Угрозы информационной безопасности интеллектуальных транспортных систем // Информационно управляющие системы. 2021. № 6. С. 2-12.

УДК 004.056

## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ

**Сейдиев Курбан Ялчинович**

Академия войск национальной гвардии

Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия

e-mail: sejdievkurban@gmail.com

**Аннотация.** В статье рассматриваются ключевые аспекты информационной безопасности объектов морской техники и инфраструктуры. Особое внимание уделяется их специфике как киберфизических систем, где интеграция IT- и OT-компонентов создает прямую угрозу физической безопасности. Анализируются современные вызовы: цифровизация, уязвимость цепочек поставок и человеческий фактор. В качестве решения предлагается системный подход, сочетающий международные стандарты (ИМО, NIST, ISA/IEC 62443) с комплексными мерами на техническом, организационном и процедурном уровнях.

**Ключевые слова:** информационная безопасность; морской транспорт; морская инфраструктура; киберриски; грузопотоки.

## INFORMATION SECURITY OF MARINE EQUIPMENT AND MARINE INFRASTRUCTURE OBJECTS

**Seydiev Kurban**

Academy of the National Guard Troops

1 Pilot Pilyutova St, St. Petersburg, 198206, Russia

e-mail: sejdievkurban@gmail.com

**Abstract.** The article examines key aspects of information security for marine equipment and infrastructure objects. Special attention is paid to their specifics as cyber-physical systems, where the integration of IT and OT components creates a direct threat to physical safety. Modern challenges are analyzed: digitalization, supply chain vulnerabilities, and the human factor. As a solution, a systematic approach is proposed, combining international standards (IMO, NIST, ISA/IEC 62443) with comprehensive measures at the technical, organizational, and procedural levels.

**Keywords:** information security; marine equipment; marine infrastructure; cyber risk; cargo flows.

Специфика объекта защиты: Объекты морской техники (судна, буровые платформы) и морской инфраструктуры (порты, системы управления движением судов, подводные кабели связи) представляют собой сложные киберфизические системы. Их ключевая особенность — тесная интеграция информационных технологий (IT) и операционных технологий (OT). Атака на IT-сегмент (например, судовую сеть) может привести к прямому физическому воздействию на OT-компоненты (главный двигатель, системы рулевого управления, балластные системы), провоцируя катастрофы [1].

Цифровизация судовых систем: Внедрение систем интегрированного мостика (IBS), электронных карт (ECDIS), систем автоматической идентификации (AIS) и спутниковой связи расширяет поверхность для атак.

Угрозы для морской инфраструктуры: Кибератаки на портовые логистические системы (например, атака вредоносного ПО NotPetya на порт Maersk) парализуют грузопотоки, а атаки на системы управления шлюзами или нефтехранилищами могут привести к экологическому ущербу [2].

Человеческий фактор: Недостаточная осведомленность экипажей и персонала портов о киберугрозах остается слабым звеном [3].

Необходимость системного подхода к защите.

Ключевую роль играют международные стандарты, прежде всего Резолюция ИМО MSC.428(98), которая обязывает судовладельцев включать управление киберрисками в существующие системы безопасности (МКУБ). Это требует реализации frameworks, таких как NIST Cybersecurity Framework или стандарты ISA/IEC 62443 для OT-систем [4].

Таким образом Обеспечение информационной безопасности объектов морской техники и инфраструктуры требует перехода от точечных решений к созданию целостных систем управления киберрисками, основанных на международных стандартах, глубоком понимании конвергенции IT и OT и постоянной адаптации к эволюции угроз. Успех в этой области является залогом безопасного, устойчивого и экономически эффективного будущего мировой морской индустрии.

## СПИСОК ЛИТЕРАТУРЫ

1. Резолюция ИМО MSC.428(98) «Меры по управлению кибербезопасностью в области морской безопасности». Международная морская организация (ИМО), 2017.
2. Рекомендации ИМО по управлению киберрисками (IMO Guidelines on Maritime Cyber Risk Management). ИМО, 2017, 2021.
3. МКУБ (International Safety Management Code) с учетом включения аспектов киберрисков в систему управления безопасностью.
4. Стандарты серии МЭК 62443 «Сети и системы промышленной автоматизации. Информационная безопасность». Применяются для АСУ ТП судов и портовой инфраструктуры.

УДК 004; 519

**ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МЕЖВЕДОМСТВЕННОГО  
ВЗАИМОДЕЙСТВИЯ ЗВЕНЬЕВ РСЧС****Синешук Юрий Иванович, Карацев Гия Георгиевич, Каиров Заур Геннадьевич**

Санкт-Петербургский университет ГПС МЧС России

Московский пр., 149, Санкт-Петербург, 196105, Россия

e-mails: sinegal53@mail.ru, giya.karatsev.82@mail.ru, zaur-kair2013@yandex.ru

**Аннотация.** Сформулированы принципы обеспечения информационной безопасности межведомственного взаимодействия звеньев РСЧС, как разновидности социотехнических систем, где взаимодействуют люди и технологии.

**Ключевые слова:** чрезвычайная ситуация; управление; межведомственное взаимодействие; информационно-аналитическое обеспечение; информационная безопасность.

**PRINCIPLES OF ENSURING INFORMATION SECURITY OF INTERDEPARTMENTAL  
INTERACTION OF THE UNIT OF THE RSChS****Sineshchuk Yuri, Karatsev Giya, Kairov Zaur**

St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia

149 Moskovskiy Av, St. Petersburg, 196105, Russia

e-mails: sinegal53@mail.ru, giya.karatsev.82@mail.ru, zaur-kair2013@yandex.ru

**Abstract.** The principles of ensuring information security of interdepartmental interaction of the RSChS units, as a type of socio-technical systems where people and technologies interact, are formulated.

**Keywords:** emergency; management; interdepartmental interaction; information and analytical support; information security.

Важным критерием, по которому можно оценить уровень готовности должностных лиц органов управления (ДЛОУ) РСЧС к выполнению возложенных на них функций и задач, можно назвать качество их информационно аналитического обеспечения (ИАО).

Качество ИАО, как правило, рассматривается с точки зрения достоверности, актуальности, адекватности и оперативности сведений, необходимых для принятия соответствующих управленческих решений.

Для ИАО деятельности ДЛОУ РСЧС по предупреждению и ликвидации чрезвычайных ситуаций создана автоматизированная информационно-управляющая система (АИУС РСЧС), построенная как территориально распределенная система республиканских, краевых, областных информационно-управляющих центров, городских и районных абонентских пунктов, объединенных государственными и ведомственными каналами связи и передачи данных, функционирование которой предусматривает интенсивное информационное взаимодействие звеньев РСЧС различного иерархического уровня [1, 2].

Концентрация больших объемов передаваемой, обобщенной и систематизированной информации в автоматизированных системах обработки информации МЧС приводит к увеличению вероятности деструктивных действий объективного и субъективного характера, связанных с ее утечкой, искажением, либо уничтожением, а значит, и к необходимости принятия мер по обеспечению безопасности информации.

Информационная безопасность (ИБ) включает в себя обеспечение конфиденциальности, целостности, доступности информации и является критически важной для эффективного решения задач по предупреждению и ликвидации ЧС. Она направлена на защиту от угроз, связанных с человеческим фактором и техническими сбоями, а также на поддержание устойчивости и надежности системы в целом [3].

В качестве основных принципов обеспечения информационной безопасности межведомственного взаимодействия звеньев РСЧС, как разновидности социотехнических систем, где взаимодействуют люди и технологии, можно назвать: аутентификация, разграничение доступа, стандартизации обмена информацией, использование защищенных каналов связи, разработки и внедрения единых политик безопасности, управление рисками, управление инцидентами, взаимодействие с пользователями, обучение и осведомленность [4].

Задача обеспечения информационной безопасности в такого рода социотехнических системах, как РСЧС, является комплексной, требующей учета как технических, так и социальных аспектов, а эффективное управление информационной безопасностью межведомственного взаимодействия звеньев РСЧС является фундаментом для успешного выполнения задач по предупреждению и ликвидации чрезвычайных ситуаций, что способствует защите населения и территории страны.

**СПИСОК ЛИТЕРАТУРЫ**

1. Иванов А. Ю., Синешук М. Ю. Организация безопасного информационного взаимодействия функциональных и территориальных подсистем РСЧС. Вестник Воронежского института ГПС МЧС России, 2013, Выпуск 4 (9), С 15-18.
2. Остapович И.Ю. К вопросу о взаимодействии Конституционного Суда РФ с высшим органом законодательной власти России // Актуальные проблемы российского права. 2015. № 8. С. 194-202.
3. Charitoudi, K., Blyth, A. A Socio-Technical Approach to Cyber Risk Management and Impact Assessment. Journal of Information Security, 04(01), 2013, 33-41.
4. Kotenko I., Sineshchuk Y., Saenko I., Optimizing secure information interaction in distributed computing systems by the sequential concessions method.: Proceedings 2020 28th Euromicro International Conference on Parallel, Distributed and Network-Based Processing, PDP 2020. 28. 2020. С. 429-432.

УДК 004; 519

**ОБОСНОВАНИЕ ТРЕБОВАНИЙ К НАДЕЖНОСТИ КАК ФАКТОРУ ОБЕСПЕЧЕНИЯ  
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ ПОЖАРНОЙ АВТОМАТИКИ****Синешук Юрий Иванович, Кубашевская Татьяна Александровна, Лебедько Елена Николаевна**

Санкт-Петербургский университет ГПС МЧС России  
Московский пр., 149, Санкт-Петербург, 196105, Россия  
e-mails: sinegal53@mail.ru, 962707@mail.ru, lebedkoelena31015@mail.ru

**Аннотация.** Предложена трактовка систем пожарной автоматики, как разновидности измерительных, информационно-управляющих систем. Обоснованы требования к их надежности в аспекте достижения требуемой эффективности функционирования и обеспечения информационной безопасности.

**Ключевые слова:** система пожарной автоматики; информационная система; процесс управления; надежность; информационная безопасность.

**JUSTIFICATION OF REQUIREMENTS TO RELIABILITY AS A FACTOR IN ENSURING  
INFORMATION SECURITY OF FIRE AUTOMATION SYSTEMS****Sineshchuk Yury, Kubashevskaya Tatyana, Lebedko Elena**

St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia  
149 Moskovskiy Av, St. Petersburg, 196105, Russia  
e-mails: sinegal53@mail.ru, 962707@mail.ru, lebedkoelena31015@mail.ru

**Abstract.** The interpretation of fire automatic systems as a type of measuring, information and control systems is proposed. The requirements for their reliability in terms of achieving the required efficiency of operation and ensuring information security are substantiated.

**Keywords:** fire automatic system; information system; management process; reliability; information security.

Современные сложные объекты защиты различного функционального назначения предполагают интеграцию многообразных средств и систем автоматизации в единое информационное пространство, в том числе это касается и систем автоматической противопожарной защиты, основу которых составляют системы пожарной автоматики (СПА). В настоящее время эти системы постоянно расширяют спектр механизмов, способных справиться не только с проявлениями опасных факторов пожара, критическими последствиями пожара, но и механизмов контроля (измерения) и обеспечения работоспособности системы, адаптивного управления функциональными процессами [1, 2].

СПА являются информационными системами, поскольку они обнаруживают, обрабатывают и передают информацию о пожаре для принятия соответствующих мер. Эти системы собирают данные с датчиков, анализируют их, и в зависимости от настроек и алгоритмов, запускают оповещение о пожаре, управляют эвакуацией, активируют системы пожаротушения и другие инженерные системы здания.

Таким образом, СПА не только обнаруживают пожар, но и управляют процессами реагирования на него, что делает их важной частью информационной инфраструктуры безопасности объекта защиты.

Учитывая, то, что реализуемый этими системами процесс управления, по своей сути, является информационным, это обстоятельство актуализирует проблему информационной безопасности СПА и надежности, как обеспечивающего ее фактора.

Надежность системы, как способность функционировать без сбоев и отказов, напрямую влияет на доступность информации. Если система ненадежна, то она может часто выходить из строя, что делает информацию недоступной для пользователей, или искажает информацию, даже если она не подвергается атакам злоумышленников. Ненадежная система может быть уязвима для атак, так как сбои и ошибки в ее работе могут быть использованы злоумышленниками.

Внедрение надежных систем пожарной автоматики и средств обеспечения их информационной безопасности является необходимым условием для решения задач предотвращения пожаров и их последствий, защиты жизни, здоровья людей и имущества от пожаров [3].

Основными требованиями обеспечения надежности СПА в процессе проектирования и эксплуатации являются: комплексный подход, адаптивность, соответствие нормативным требованиям, оценка и прогнозирование рисков, использование современных методов и технологий, выбор надежного оборудования, модульность и резервирование, регулярная диагностика и обслуживание [4, 5].

Можно сказать, что надежность и информационная безопасность взаимосвязаны, и обеспечение надежности является важным шагом на пути к обеспечению безопасности информации.

**СПИСОК ЛИТЕРАТУРЫ**

1. Соколов С. В., Костюченко Д. В. Эффективность средств пожарной автоматики на пожарах в жилых домах // Пожаровзрывобезопасность / Fire and Explosion Safety. 2014. Т. 23, № 6. С. 70–75.
2. Плоткин, Б. К. Безопасность жизнедеятельности: теория надежности и управление рисками // Вестник факультета управления СПбГЭУ. 2017. № 1–2. С. 236–241.
3. Основы теории надежности : Учебник / А. В. Чепурин [и др.]. Москва : Типография ПМГ, 2023. 232 с.
4. L. Fiorentini, P. Cancelliere Fire Protection Systems functional safety requirements in performance-based design: proposed workflow and a simple case application // Journal of Physics: Conference Series: Vol. 2885, № 1, p. 012088 2024.
5. Богуцкий С.Ю., Синешук Ю.И. Методика оценки функциональной безопасности системы пожарной сигнализации на основе информационно-логической модели. Проблемы управления рисками в техносфере. 2025. № 2 (74). С. 118-129.

УДК 351.746.2

**ГНОСЕОЛОГИЯ И ПОЗНАНИЕ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ:  
КАК МЫ ПОЗНАЁМ КИБЕРУГРОЗЫ****Ставицкий Данил Владимирович, Лукьянова Александра Вячеславна**

Академия войск национальной гвардии

Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия

e-mails: stavitskiydv@spvi.ru, blacalex@yandex.ru

**Аннотация.** В статье рассматриваются процессы исследования познания в информационной безопасности через призму ключевых гносеологических концепций: границ достоверности, природы истины, роли субъекта и объекта познания.

**Ключевые слова:** информационная безопасность; объект познания; субъект познания; технологии.

**GNOSEOLOGY AND COGNITION IN THE SPHERE OF INFORMATION SECURITY:  
HOW WE UNDERSTAND CYBER THREATS****Stavitsky Danil, Lukyanova Alexandra**

Academy of the National Guard Troops

1 Pilot Pilyutova St, St. Petersburg, 198206, Russia

e-mails: stavitskiydv@spvi.ru, blacalex@yandex.ru

**Abstract.** The article examines the processes of research into knowledge in information security through the prism of key epistemological concepts: the boundaries of reliability, the nature of truth, the role of the subject and object of knowledge.

**Keywords:** information security; object of knowledge; subject of knowledge; technologies.

Информационная безопасность (ИБ) традиционно воспринимается как сугубо техническая область, царство программистов, криптографов и сетевиков. Однако в её основе лежит фундаментальный философский вопрос: как мы познаём цифровую реальность и можем ли мы быть уверены в её достоверности? Гносеология, или теория познания, изучающая природу, методы и ограничения человеческого знания, предлагает мощный инструментарий для анализа вызовов современного киберпространства [1].

В классической гносеологии чётко разделяются субъект (тот, кто познаёт) и объект (то, что познаётся). В информационной безопасности это разделение крайне проблематично.

Объект познания — это гибридная цифрово-физическая система: сетевой трафик, логи серверов, поведение пользователей, исходный код, конфигурации. Этот объект нестабилен, изменчив и часто намеренно искажается противником (атакующим).

Субъект познания — это специалист по ИБ (аналитик, исследователь). Но его познавательные возможности ограничены опосредованностью и теоретической нагруженностью наблюдения.

Опосредованность — мы не «видим» атаку напрямую. Мы познаём её через интерпретацию данных: записи в логах, срабатывания систем обнаружения (SIEM), показания датчиков. Эти данные — не сама реальность, а её модель, часто неполная и искажённая.

Теоретическая нагруженность наблюдения. Аналитик видит не просто «странный пакет». Он видит «возможный сканер уязвимостей» или «признак АРТ-атаки». Его восприятие определяется его предыдущим опытом, знаниями и используемыми теориями (например, моделью угроз). Это делает процесс познания крайне субъективным [2].

Методы познания в ИБ: от эмпирики к абдукции. Эмпиризм (опыт), основа ИБ — это сбор и анализ данных (логов, артефактов, образцов вредоносного ПО). Без эмпирического наблюдения познание невозможно. Однако, как показал ещё Дэвид Юм, опыт не может дать всеобщее и необходимое знание: «то, что атака прошла вчера 100 раз, не означает, что она пройдёт завтра».

Рационализм (разум) — использование логических моделей, формальных методов верификации, математических основ криптографии. Разум позволяет выстраивать теории и предсказывать угрозы.

Абдуктивное мышление (вывод к лучшему объяснению) — это ключевой метод познания в расследовании инцидентов (Digital Forensics and Incident Response — DFIR). Аналитик видит набор разрозненных артефактов (следы) и формирует гипотезу, которая наилучшим образом объясняет их происхождение. Например: «На сервере А найден бэкдор, с сервера В идёт подозрительный исходящий трафик. Наиболее вероятное объяснение — злоумышленник скомпрометировал сервер А и использует его для атаки на сервер В» [3].

Таким образом, информационная безопасность — это не только борьба с хакерами, но и постоянная борьба с собственным незнанием. Гносеология даёт нам философский фундамент, чтобы вести эту борьбу более осознанно и эффективно.

**СПИСОК ЛИТЕРАТУРЫ**

1. Патаракин Е.Д. Сетевые сообщества и обучение. М.: НИИ школьных технологий, 2010. 176 с.
2. Ставицкий Д.В., Фетисов А.В. «Значение профессиональных компетенций и компетентности военных специалистов при организации образовательной деятельности». Статья. ОТЖ №2, 2019 г. С. 5-6.
3. Цеханович, Д.Б., Панкратов, В.С. Каким быть современному военному образованию / Армейский сборник. 2022. № 12. Электронный ресурс: <http://army.ric.mil.ru/Stati/item/456129/> (дата обращения: 09.09.2025).

УДК 351.746.2

**ЗАЩИТА ИНФОРМАЦИИ В ВЫСШИХ ВОЕННО-ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЯХ****Ставицкий Данил Владимирович, Минец Вячеслав Николаевич**

Академия войск национальной гвардии

Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия

e-mail: stavitskiydv@spvi.ru, minetsvn@rosgvard.ru

**Аннотация.** В статье рассматриваются ключевые аспекты системы защиты информации в высших военно-образовательных учреждениях. Анализируются уникальные угрозы информационной безопасности, специфика защищаемых сведений и комплексный подход к построению эффективной системы, сочетающий технические, организационные и человеческие факторы.

**Ключевые слова:** категории защищаемой информации, информационная безопасность, технологии; технические средства защиты; утечка информации.

**INFORMATION PROTECTION IN HIGHER MILITARY EDUCATIONAL INSTITUTIONS****Stavitsky Danil, Minets Vyacheslav**

Academy of the National Guard Troops

1 Pilot Pilyutova St, St. Petersburg, 198206, Russia

e-mail: stavitskiydv@spvi.ru, minetsvn@rosgvard.ru

**Abstract.** The article examines key aspects of the information security system in higher military educational institutions. Unique threats to information security, the specifics of protected information, and a comprehensive approach to building an effective system that combines technical, organizational, and human factors are analyzed.

**Keywords:** categories of protected information, information security, technologies; technical means of protection; information leak.

Актуальность темы связана с необходимостью активного функционирования информационных систем в высших военно-образовательных учреждениях, осуществляющих обработку персональных данных, делопроизводство, программы обучения. В связи с этим защита информации в стенах этих учреждений выходит за рамки стандартной и превращается в задачу государственной важности. Её решение требует особого, многогранного подхода, интегрированного во все процессы деятельности вуза. [1].

Защитить данную информацию возможно при создании сильной организационной защиты информации — это регламентация деятельности и взаимоотношений исполнителей на нормативно-правовой основе. [2].

Защита информации строится на принципах системности и непрерывности и включает несколько взаимосвязанных уровней. Нормативно-правовая и организационная основа: а) Режим секретности: четкое определение степени секретности сведений, градация доступа, ведение секретного делопроизводства. б) Регламентация всех процессов: в) Разработка и неукоснительное соблюдение инструкций по работе с информацией, использованию съемных носителей, правил парольной политики, порядка доступа в интернет. г) Кадровая работа: тщательная проверка персонала и курсантов при допуске к секретным сведениям (форма допуска), регулярные инструктажи, создание атмосферы ответственности.

Технические средства защиты: а) Физическая охрана периметра и помещений: контроль доступа с использованием пропусков, видеонаблюдение, охрана. б) Защита от утечки информации: использование сертифицированной техники, экранирование помещений, подавители сотовой связи в аудиториях для проведения закрытых занятий. в) Аттестованные автоматизированные системы: создание изолированных защищенных сетевых сегментов для обработки информации ограниченного доступа, не имеющих выхода в глобальный интернет. г) Средства криптографической защиты: шифрование каналов связи и данных для обеспечения конфиденциальности и целостности передаваемой информации. д) Средства защиты от несанкционированного доступа: Межсетевые экраны, системы обнаружения и предотвращения вторжений, системы для предотвращения утечек. е) Чистый стол: правило, обязывающее сотрудников убирать все документы при окончании рабочего дня.

Работа с персоналом и курсантами: а) Самый слабый элемент в любой системе защиты — человек. б) Воспитанию культуры безопасности: формирование у каждого участника учебного процесса личной ответственности за сохранность государственной тайны. в) Контролю соблюдения: жесткая дисциплина и санкции за нарушение установленных правил. [3].

Таким образом, защита информации в высших военно-образовательных учреждениях — это не просто набор технических средств и инструкций. Это сложная, динамично развивающаяся система, глубоко интегрированная в учебный, научный и административный процессы. Её эффективность определяется триадой: технологии, регламенты и человек.

**СПИСОК ЛИТЕРАТУРЫ**

1. Терехов, А. В. Правовые аспекты использования цифровых технологий и обеспечения кибербезопасности / А. В. Терехов, А. М. Арестова // Инновационная юриспруденция: Вопросы теории и практики : сб. науч. тр. по материалам II Междунар. науч.-практ. конф. Тамбов: Издательство Першина Р.В., 2022. С. 85-89.
2. Ставицкий Д.В., Фетисов А.В «Значение профессиональных компетенций и компетентности военных специалистов при организации образовательной деятельности». Статья. ОТЖ №2, 2019 г. С. 5-6.
3. Защита компьютерной информации : учебное пособие / А. В. Терехов, В. Н. Чернышов, А. В. Селезнев, И. П. Рак. Тамбов : Изд-во ТГТУ, 2003. 80 с.

УДК 351.746.2

**ПРАВОВОЕ ОБЕСПЕЧЕНИЕ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ:  
ОСНОВЫ, ВЫЗОВЫ И ТЕНДЕНЦИИ****Ставицкий Данил Владимирович, Фролова Лариса Валерьевна**

Академия войск национальной гвардии

Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия

e-mails: stavitskiydv@spvi.ru, frolovalora71@yandex.ru

**Аннотация.** В современном цифровом мире информация стала ключевым активом, источником развития и одновременно уязвимым местом для государств, компаний и граждан. Возрастающие угрозы киберпреступности, утечки данных, кибертерроризма и цифрового шпионажа делают невозможным обеспечение безопасности исключительно техническими средствами.

**Ключевые слова:** информационные технологии; гуманитарное образование; цифровизация; дистанционное обучение; педагогические методы; цифровая грамотность.

**LEGAL SUPPORT IN THE SPHERE OF INFORMATION SECURITY:  
FUNDAMENTALS, CHALLENGES AND TRENDS****Stavitsky Danil, Frolova Larisa**

Academy of the National Guard Troops

1 Pilot Pilyutova St, St. Petersburg, 198206, Russia

e-mails: stavitskiydv@spvi.ru, frolovalora71@yandex.ru

**Abstract.** In today's digital world, information has become a key asset, a source of development and, at the same time, a vulnerable spot for states, companies and citizens. Growing threats of cybercrime, data leakage, cyberterrorism and digital espionage make it impossible to ensure security solely by technical means.

**Keywords:** information technology; humanitarian education; digitalization; distance learning; pedagogical methods; digital literacy.

В настоящее время в информационных правоотношениях появляются ранее неизвестные праву субъекты и объекты, методы информационно-правового воздействия, перестраиваются общепризнанные и появляются новые общественные отношения и связи. В связи с этим требуется правовая база, которая определяла бы правила игры, права и обязанности всех участников цифрового пространства, а также устанавливала меру ответственности за нарушения. Правовое обеспечение информационной безопасности (ИБ) — это комплекс нормативных правовых актов, регулирующих общественные отношения, связанные с созданием, использованием, распространением и защитой информации, информационных систем и технологий [1].

Правовое обеспечение в сфере ИБ представляет собой многоуровневую систему, основанную на иерархии нормативных актов.

Международный уровень включает конвенции, соглашения и директивы, которые формируют общие подходы к регулированию киберпространства. Ключевым примером являются

— будапештская конвенция о киберпреступности (2001 г.) — первый международный договор, направленный на борьбу с компьютерными преступлениями путем гармонизации национального законодательства.

— директива — обязывает страны-члены ЕС повышать уровень своей кибербезопасности и ужесточает требования к операторам важнейших услуг.

— регламент ЕС (Общий регламент по защите данных) — устанавливает строгие правила обработки и защиты персональных данных граждан ЕС [2].

Законодательство в области ИБ базируется на нескольких основополагающих принципах.

Первый принцип — это законность. Все меры по защите информации должны осуществляться в строгом соответствии с законом. Второй принцип — баланс интересов — баланс между безопасностью государства, интересами бизнеса и правами личности на приватность.

Следующий принцип — системность и комплексность. Защита информации должна быть всеобъемлющей, объединяя правовые, организационные и технические меры. Важный принцип — ответственность, предполагающий четкое определение ответственности за нарушения установленных правил.

Последний принцип — разграничение доступа. Установление правил доступа к информации в зависимости от ее конфиденциальности и полномочий субъекта [3].

Таким образом, правовое обеспечение информационной безопасности является динамично развивающейся и критически важной отраслью права. Оно выступает не просто набором запретов, а основой для построения безопасного и доверительного цифрового пространства.

**СПИСОК ЛИТЕРАТУРЫ**

1. Патаракин Е.Д. Сетевые сообщества и обучение. М.: НИИ школьных технологий, 2010. 176 с. С. 85-89.
2. Ставицкий Д.В., Фетисов А. В. «Значение профессиональных компетенций и компетентности военных специалистов при организации образовательной деятельности». Статья. ОТЖ №2, 2019 г. С. 5-6.
3. Карпенко О.М., Вайндорф-Сысоева М.Е. Цифровая дидактика: риски и возможности // Высшее образование в России. 2020. Т. 29. № 12. С. 21-31.



УДК 004.056.5

**ОБЕСПЕЧЕНИЕ ЛИЧНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВОЕННОСЛУЖАЩИХ  
(СОТРУДНИКОВ) СТРУКТУРНЫХ ПОДРАЗДЕЛЕНИЙ СИЛОВЫХ ВЕДОМСТВ****Сурков Алексей Сергеевич, Баранов Андрей Александрович**

Академия войск национальной гвардии

Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия

e-mails: aleksej.surkov.90@bk.ru, andrejbaranov43504@mail.ru

**Аннотация.** В современном мире информационные технологии играют важную роль в деятельности государственных служащих. В результате активного развития информационных технологий и ростом объема обрабатываемых данных увеличивается риск их утечки, что может нанести ущерб не только отдельно взятому человеку, но и государству в целом. Поэтому обеспечение личной информационной безопасности и повышение информационной грамотности госслужащих является приоритетной задачей для государственных структур.

**Ключевые слова:** информационная безопасность; информационные технологии; государственные структуры.

**ENSURING PERSONAL INFORMATION SECURITY OF MILITARY PERSONNEL (EMPLOYEES)  
OF STRUCTURAL UNITS OF SECURITY AGENCIES****Surkov Aleksey, Baranov Andrew**

Academy of the National Guard Troops

1 Pilot Pilyutova St, St. Petersburg, 198206, Russia

e-mails: aleksej.surkov.90@bk.ru, andrejbaranov43504@mail.ru

**Abstract.** In the modern world, information technology plays an important role in the activities of servants. As a result of the active development of information technology and the growth of the volume of processed data, the risk of their leakage increases, which can cause damage not only to an individual but also to the state as a whole. Therefore, ensuring personal information security and improving the information literacy of civil servants is a priority for government agencies.

**Keywords:** information security; mathematical methods; government structures.

Актуальность темы определяется тем, что госслужащие ежедневно работают с конфиденциальными данными, доступ к которым должен быть строго ограничен и защищен. Нарушение безопасности может привести к утечке информации, что в современных условиях может нести непосредственную угрозу не только жизни и здоровью граждан, но и государственной безопасности и стабильности [1].

Самыми распространенными угрозами на данный момент являются вербовка военнослужащих (сотрудников) структурных подразделений силовых ведомств и государственных служащих иностранными спецслужбами путем шантажа и подкупа. Злоумышленники и сотрудники иностранных спецслужб по причине безответственности, халатности или некомпетентности лиц, имеющих доступ к сведениям, составляющим государственную тайну, выявляют таковые и, оказывая на них давление, вынуждают нарушать режим секретности, а также сподвигают к таким деяниям как умышленная порча госимущества, саботаж и государственная измена [2].

Интересующая нас тематика, в первую очередь, связана с определением направлений и методик разработки политики информационной безопасности военнослужащих (сотрудников) структурных подразделений силовых ведомств и государственных служащих.

Для решения ряда частных задач в этой области необходимо обучать сотрудников правилам информационной грамотности и безопасности. Госслужащие обязаны знать о возможных угрозах, уметь распознавать мошеннические схемы и соблюдать правила безопасного использования информационных систем. Регулярные тренинги и повышение квалификации помогают снизить риск ошибок и неосторожных действий.

Также необходимо внедрять уровневую проверку для доступа в режимные помещения. Ограничение прав доступа и контроль за использованием устройств позволяют минимизировать вероятность внутренней утечки информации. Важным элементом является и физическая безопасность — хранение устройств в защищенных местах с использованием технических средств контроля [3].

Обеспечение личной информационной безопасности госслужащих требует системного подхода, включающего технические меры, обучение персонала и внутренние регламенты. Необходимо развивать среди сотрудников чувство личной ответственности к неразглашению сведений составляющих государственную тайну и персональным данным третьих лиц.

**СПИСОК ЛИТЕРАТУРЫ**

1. Директива Росгвардии от 28 октября 2021 г. № Д-2 «О приоритетных направлениях деятельности войск национальной гвардии Российской Федерации в 2022 году» // Сайт Росгвардии. URL: <https://rosguard.gov.ru/> (дата обращения: 20.07.2025).
2. Доктрина информационной безопасности Российской Федерации // URL: <https://rg.ru/documents/2016/12/06/doktrina-infobezobasnost-site-dok.html> (дата обращения: 20.07.2025).
3. Примакин, А.И. Практический опыт применения инновационных технологий при подготовке сотрудников в области обеспечения защиты информации правоохранительных органов / Информационные технологии, связь и защита информации МВД России 2012. Выпуск второй. 2012. С. 90-92.

УДК 004.056:34

**ПРАВОВЫЕ ПОСЛЕДСТВИЯ УТЕЧЕК ПЕРСОНАЛЬНЫХ ДАННЫХ****Тищенко Ирина Вячеславовна**

Военная ордена Жукова академия войск национальной гвардии Российской Федерации  
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия  
e-mail: ira\_koroleva@inbox.ru

**Аннотация.** В данной работе рассматривается комплексная система правового обеспечения информационной безопасности в Российской Федерации. Анализируются ключевые элементы системы: нормативно-правовая база, уголовная ответственность за киберпреступления, защита персональных данных, а также проблемы правоприменения и международно-правового регулирования.

**Ключевые слова:** информационная безопасность, защита, профилактика.

**LEGAL CONSEQUENCES OF PERSONAL DATA BREACHES****Tishchenko Irina**

Military Order of Zhukov Academy of the National Guard Troops of the Russian Federation  
Pilyutov Pilot Street, 1, Saint Petersburg, 198206, Russia  
e-mail: ira\_koroleva@inbox.ru

**Abstract.** This paper examines the comprehensive system of legal support for information security in the Russian Federation. It analyzes the key elements of the system, including the legal framework, criminal liability for cybercrimes, protection of personal data, and issues related to law enforcement and international legal regulation.

**Keywords:** information security, protection, and prevention.

Административная ответственность (ст. 13.11 КоАП РФ) является наиболее частым последствием. Штрафы для юридических лиц могут достигать сотен тысяч рублей (до 500 тыс. за обработку ПДн без согласия или до 1 млн. руб. по некоторым частям). При этом, важным нововведением является обязанность оператора уведомить Роскомнадзор и субъектов ПДн об утечке, неисполнение которой также влечет отдельный штраф.

Гражданско-правовая ответственность субъекты ПДн, чьи права нарушены, вправе требовать возмещения убытков (как реального ущерба, так и упущенной выгоды) и компенсации морального вреда (ст. 151 ГК РФ). Суммы компенсаций в судебной практике растут, формируя серьезные финансовые издержки для компаний.

Уголовная ответственность (ст. 137 УК РФ) применяется реже, но в случаях умышленного распространения сведений о частной жизни без согласия лица может привести к лишению свободы для должностных лиц компании. Это создает персональные риски для руководителей и IT-специалистов [3].

Защита прав граждан при утечках остается недостаточно эффективной, несмотря на формальное закрепление механизмов.

Проблема доказывания: гражданину крайне сложно доказать размер причиненных убытков и прямую причинно-следственную связь между утечкой и наступившими негативными последствиями (например, взломом банковской карты).

Низкая правовая грамотность: многие пострадавшие не знают о своих правах или не готовы обращаться в суд из-за сложности и длительности процесса [1].

Реактивный характер защиты: права граждан защищаются после наступления инцидента, в то время как превентивные механизмы (такие как эффективный контроль со стороны Роскомнадзора) развиты слабее.

Таким образом правовые последствия утечек персональных данных в России эволюционируют в сторону создания сбалансированной системы: с одной стороны, ужесточается и диверсифицируется ответственность компаний, делая халатное отношение к безопасности ПДн экономически невыгодным, а с другой – постепенно формируются судебные механизмы, позволяющие гражданам эффективно защищать свои нарушенные права.

Однако для достижения полной эффективности необходимы дальнейшие шаги: повышение прозрачности расследования инцидентов, популяризация инструментов коллективных исков и развитие страхования киберрисков, что позволит перевести защиту прав граждан на более проактивный уровень [2].

**СПИСОК ЛИТЕРАТУРЫ**

1. Грачев Г.В., Мельник И.К. Манипулирование личностью: Организация, способы и технологии информационно-психологического воздействия. – М.: Алгоритм, 2015. – 384 с. (Фундаментальная работа по технологиям манипуляции сознанием).
2. Зиновьев А.А. Запад: Феномен западнизма. – М.: Эксмо, 2007. – 512 с. (Работа раскрывает методы информационно-психологического воздействия в масштабах общества, тема эрозии идентичности).
3. Сундиев И.Ю. Анатомия информационной войны: Психологические операции в современном мире. – М.: Книжный мир, 2019. – 320 с. (Актуальное исследование, посвященное конкретным механизмам ведения информационной войны против личности и общества).

УДК 341.4

**СРАВНИТЕЛЬНЫЙ АНАЛИЗ УГОЛОВНО-ПРАВОВОЙ ЗАЩИТЫ ОТ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ В ИНДИИ И В РОССИИ****Хазинурова Екатерина Андреевна**

Санкт-Петербургский университет МВД России

Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия

e-mail: ekaterina.simakova.2001@yandex.ru

**Аннотация.** В статье проводится сравнительный анализ уголовно-правовых механизмов противодействия компьютерным преступлениям в Индии и Российской Федерации. Рассматриваются особенности законодательства двух стран, а также перспективы реформирования правовой базы в условиях цифровизации общества. Отдельное внимание уделено проблемам защиты персональных данных и перспективам международного сотрудничества в сфере кибербезопасности.

**Ключевые слова:** компьютерные преступления; Индия; международное сотрудничество; персональные данные; правовой механизм.

**COMPARATIVE ANALYSIS OF CRIMINAL LAW PROTECTION FROM COMPUTER CRIMES IN INDIA AND IN RUSSIA****Khazinurova Ekaterina**

St. Petersburg University of the Ministry of Internal Affairs of Russia

1 Pilot Pilyutova St, St. Petersburg, 198206, Russia

e-mail: ekaterina.simakova.2001@yandex.ru

**Abstract.** The article provides a comparative analysis of the criminal law mechanisms for countering computer crimes in India and the Russian Federation. The features of the legislation of the two countries, as well as the prospects for reforming the legal framework in the context of digitalization, are examined. Special attention is paid to the issues of personal data protection and the prospects for international cooperation in the field of cybersecurity.

**Keywords:** computer crimes; India; international cooperation; personal data; legal mechanism.

В отчете ООН от 20 июня 2024 года указано, что за 2023 год злоумышленники в результате компьютерных преступлений получили 1,1 миллиарда долларов США [1]. Вредоносные программы, вирусы-вымогатели, фишинг и атаки типа «отказ в обслуживании», используются для совершения преступлений на государственные и частные сети, угрожая важнейшим объектам инфраструктуры и общественной безопасности.

Индия занимает лидирующие позиции в цифровом пространстве, располагая второй по величине интернет-аудиторией в мире после Китая — свыше 560 миллионов пользователей. На страну приходится рекордные 21% глобального прироста интернет-аудитории: за 2019 год количество индийских пользователей сети увеличилось почти на 100 миллионов — максимальный показатель среди всех стран мира.

Индийская правовая система характеризуется дуалистическим подходом к криминализации противоправных деяний, предполагающим применение уголовно-правовых санкций как на основании норм Индийского уголовного кодекса (Indian Penal Code, 1860), так и посредством специального законодательства. Данная правовая модель демонстрирует синтез классических принципов уголовного права с отраслевым нормотворчеством, адаптированным к специфике отдельных видов преступной деятельности.

Основным нормативным актом в сфере информационной безопасности в Индии является Information Technology Act, 2000 (с поправками 2008 г.), который, в отличие от Уголовного кодекса Российской Федерации, носит комплексный характер и регулирует не только уголовные, но и гражданско-правовые дела [2]. Данный документ устанавливает правовые основы для электронного документооборота, использования цифровых подписей, а также определяет состав преступлений в области информационной безопасности. Кроме того, в нем содержатся положения, касающиеся защиты персональных данных и предусматривающие ответственность за киберпреступления.

К основным составам компьютерных преступлений, в соответствии с ИТА относятся:

- отправка оскорбительных сообщений через службы связи;
- недобросовестное получение похищенных компьютерных ресурсов или устройств связи;
- кража персональных данных;
- мошенничество с использованием дипфейков;
- нарушение конфиденциальности;
- кибертерроризм;
- распространение или передача в электронной форме материалов непристойного характера.

Бурный рост интернет-аудитории в Индии, которая по прогнозам достигнет 900 миллионов пользователей к 2026 году, происходит одновременно с недостаточно развитой инфраструктурой кибербезопасности. В Индии действует система цифровой идентификации Aadhaar [3]. Она считается крупнейшей в мире базой биометрических данных, объединяющей отпечатки пальцев, скан радужки глаза и иных персональных данных. Система стала важным инструментом для обеспечения доступа населения к социальным услугам, банковским операциям и электронным сервисам государства. Однако столь масштабная концентрация персональных данных

сопровождается повышенными рисками: в последние годы неоднократно фиксировались факты несанкционированного доступа к базе, массовые утечки информации и случаи использования похищенных сведений для финансового мошенничества.

В российском законодательстве уголовная ответственность за компьютерные преступления предусмотрена главой 28 «Преступления в сфере компьютерной информации» Уголовного кодекса Российской Федерации [4]:

- ст. 272 УК РФ — неправомерный доступ к компьютерной информации;
- ст. 272.1 УК РФ — незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения;
- ст. 273 УК РФ — создание, использование и распространение вредоносных компьютерных программ;
- ст. 274 УК РФ — нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей;
- ст. 274.1 УК РФ — неправомерное воздействие на критическую информационную инфраструктуру РФ.

Помимо главы 28, вопросы борьбы с киберпреступностью затрагиваются в ст. 159<sup>6</sup> УК РФ (мошенничество в сфере компьютерной информации), ст. 137 УК РФ (нарушение неприкосновенности частной жизни с использованием компьютерных технологий), а также в нормах об экстремизме и терроризме, применяемых в случаях совершения преступлений в сети Интернет.

Очевидно, что российское законодательство ориентировано преимущественно на защиту компьютерной информации и инфраструктуры, в то время как индийская модель (ИТА, 2000) шире, и в том числе охватывает гражданско-правовые и административные аспекты.

Основной целью реформирования уголовно-правовых механизмов противодействия компьютерным преступлениям должно стать создание гибкой правовой системы. Данная система должна не только адекватно реагировать на существующие угрозы, но и обладать способностью адаптироваться к новым формам киберпреступности, сохраняя при этом баланс между требованиями безопасности и защитой фундаментальных прав человека.

Для российской правовой системы первоочередное значение приобретает глубокая модернизация уголовного законодательства. Необходимо введение новых составов преступлений, учитывающих современные технологические реалии, таких как кибертерроризм с использованием искусственного интеллекта или манипуляции алгоритмами социальных сетей.

Особого внимания заслуживает вопрос определения правового статуса цифровой валюты и криптоактивов как объекта преступных посягательств. Параллельно требуется развитие альтернативных механизмов международного сотрудничества, в частности через углубление взаимодействия в рамках БРИКС и ШОС, а также создание совместных с Индией баз данных о киберпреступниках.

Для России полезен индийский опыт быстрой блокировки незаконного контента и регулирования деятельности цифровых ресурсов, а для Индии — российский опыт систематизации уголовно-правовых норм в сфере компьютерных преступлений. В законодательстве Индии существуют не урегулированные или не в полной мере урегулированные вопросы, среди них, защита интеллектуальных прав на контент в сети «Интернет», основания и условия ограничения доступа к сети «Интернет» для граждан, условия безопасности биометрических персональных данных [5].

Индийскому законодательству следует сосредоточиться на ускорении цифровой трансформации правоохранительной системы. Перспективным направлением могло бы стать создание специализированных судов, а также введение обязательной сертификации программного обеспечения для государственных учреждений.

Ключевой принцип реформирования — переход от реактивной к проактивной модели правовой защиты, когда упор делается не на наказание за совершенные преступления, а на их предупреждение и минимизацию последствий от их реализации. Особое значение приобретает развитие образовательных инициатив, направленных на подготовку сотрудников органов внутренних дел, обладающих как правовыми, так и техническими компетенциями.

Перспективным направлением российско-индийского сотрудничества в данной сфере могла бы стать совместная разработка правовых механизмов регулирования новых технологий. Пилотные проекты в рамках объединений БРИКС могли бы стать площадкой для апробации инновационных подходов к уголовно-правовой защите от компьютерных преступлений, сочетающих лучшие практики обеих стран.

#### СПИСОК ЛИТЕРАТУРЫ

1. Организация Объединенных Наций. Совет Безопасности. 9662-е заседание. Поддержание международного мира и безопасности. Противодействие меняющимся угрозам в киберпространстве. [Электронный ресурс]. URL: <https://webtv.un.org/ru/asset/k1w/k1w5v32dkj> (дата обращения: 20.07.2025).
2. Information Technology Act, 2000 (as amended in 2008). Government of India.
3. Чем в России полезен опыт крупнейшей биометрической системы в мире [Электронный ресурс]. URL: <https://www.marksworld.ru/blog/chem-v-rossii-polezen-opyt-krupneyshey-biometricheskoj-sistemy-v-mire/> (дата обращения: 21.07.2025).
4. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ: в ред. Федерального закона от 28 декабря 2024 г. № 515-ФЗ // Собрание законодательства Российской Федерации. 2024. № 53, ч. 1. Ст. 8525.
5. Республика Индия [Электронный ресурс]. URL: <https://rdc.grfc.ru/2020/10/india/> (дата обращения: 22.07.2025).



## БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

УДК 004.056

### ОБНАРУЖЕНИЕ АНОМАЛИЙ В ИНФОРМАЦИОННЫХ СИСТЕМАХ НА ОСНОВЕ ГЕТЕРОГЕННЫХ ГРАФОВЫХ НЕЙРОННЫХ СЕТЕЙ И БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ

Абраменко Георгий Тимофеевич<sup>1</sup>, Котенко Игорь Витальевич<sup>2</sup>

<sup>1</sup> Университет ИТМО

Кронверкский пр., 49, Санкт-Петербург, 197101, Россия

<sup>2</sup> СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия

e-mails: gtabramenko@itmo.ru, ivkote@comsec.spb.ru

**Аннотация.** В работе предложен подход к обнаружению аномального поведения в информационных системах на основе сочетания гетерогенных графовых нейронных сетей (HGNN) и больших языковых моделей (LLM). Данный подход позволяет повысить точность обнаружения сложных атак, используя контекстуальный анализ и выявление скрытых взаимосвязей между событиями.

**Ключевые слова:** информационная безопасность; обнаружение аномалий; гетерогенные графовые нейронные сети; большие языковые модели; машинное обучение.

### ANOMALY DETECTION IN INFORMATION SYSTEMS BASED ON HETEROGENEOUS GRAPH NEURAL NETWORKS AND LARGE LANGUAGE MODELS

Abramenko Georgii<sup>1</sup>, Kotenko Igor<sup>2</sup>

<sup>1</sup> ITMO University

49 Kronverksky Av, St. Petersburg, 197101, Russia

<sup>2</sup> St. Petersburg Federal Research Center of the Russian Academy of Sciences

39 14th Line VO, St. Petersburg, 199178, Russia

e-mails: gtabramenko@itmo.ru, ivkote@comsec.spb.ru

**Abstract.** The paper proposes an approach for detecting anomalous behavior in information systems based on a combination of heterogeneous graph neural networks (HGNN) and large language models (LLM). This approach increases the accuracy of detecting complex attacks by utilizing contextual analysis and identifying hidden interconnections between events.

**Keywords:** information security; anomaly detection; heterogeneous graph neural networks; large language models; machine learning.

В информационных системах своевременное обнаружение аномалий имеет критическое значение для предотвращения инцидентов. Традиционно для этих целей используются сигнатурные и регламентные методы [1], а также аномалийно-ориентированные подходы для облачных инфраструктур [2]. Однако современные сложные распределенные атаки, включая целевые (APT), требуют более интеллектуальных средств анализа. Перспективным направлением является применение гетерогенных графовых нейронных сетей (HGNN) и больших языковых моделей (LLM) для выявления сложных аномальных паттернов.

HGNN позволяют моделировать структуру событий безопасности в виде графов, где узлы и ребра представляют различные типы сущностей (пользователи, узлы сети, процессы, файлы и др.) и их взаимодействия, что даёт возможность обнаруживать скрытые взаимосвязи между событиями. Это подтверждается успешным применением метода OC-DHetGNN для выявления атак по графам процессов в HIDS [3].

В свою очередь, LLM, обученные на масштабных многоязычных корпусах текстов, способны понимать семантический контекст событий и выявлять новые, ранее не встречавшиеся угрозы без ручного обновления сигнатур. В недавних исследованиях показано, что такие модели, кодируя последовательности системных событий в семантически богатые векторные представления, эффективно обнаруживают малозаметные атаки типа APT [4].

В предлагаемой архитектуре модуль HGNN анализирует структурные зависимости событий (например, связи между субъектами, узлами сети, процессами и файлами), тогда как модуль LLM оценивает содержательный (семантический) контекст, включая текстовые поля (журналы, сообщения).

Для языковой модели используются действительно открытые решения, например, Llama или Mistral, которые распространяются на условиях открытой лицензии и подходят для мультязычного анализа. Таким образом реализуется мультимодальный анализ инцидентов: графовая модель обрабатывает структуру, а языковая модель — содержание, объединяя эти аспекты для более эффективного и объяснимого выявления аномалий.

Предложенный подход включает следующие этапы:

1. Сбор данных. Агрегируются события информационной безопасности из разнотипных источников: журналы операционных систем, сетевые потоки, системные вызовы, аудиты приложений и облачных сервисов.
2. Построение гетерогенного графа. Формируется граф, где узлы представляют сущности (пользователь, процесс, файл, IP-адрес и пр.), а рёбра — их взаимодействия; каждому элементу присваиваются временные и контекстные атрибуты.
3. Графовая обработка HGNN. Гетерогенная графовая нейросеть извлекает эмбединги узлов/рёбер и вычисляет структурную аномальность, выявляя отклоняющиеся подграфы.
4. Семантический анализ LLM. Подозрительные подграфы и связанные текстовые данные (команды, URL, сообщения) поступают в LLM, которая оценивает семантику действий и уточняет вероятность угрозы.
5. Интегрированный скоринг и реагирование. Результаты HGNN и LLM агрегируются в единый показатель риска; генерируются объяснения и рекомендации для SOC, при необходимости автоматически инициируются меры реагирования.

В частности, LLM обеспечивает генерацию понятных описаний обнаруженных отклонений и рекомендаций по реагированию [5], повышая интерпретируемость работы системы и облегчая анализ инцидентов специалистами.

Предлагаемый подход может быть востребован для мониторинга безопасности различных облачных инфраструктур и корпоративных сетей [6], а также контейнеризированных сред, например, платформ Docker/Kubernetes, обеспечивая проактивное обнаружение известных и ранее неизвестных кибератак на основе как структурных, так и содержательных признаков событий. Также он может быть применен для проектирования защищенных систем и устройств, в том числе встроженных [7, 8].

*Исследование выполнено за счет гранта Российского научного фонда № 25-11-20028, <https://rscf.ru/project/25-11-20028/>.*

#### СПИСОК ЛИТЕРАТУРЫ

1. Котенко И. В., Мельник М. В. Обнаружение атак и аномалий в контейнерных системах: подходы на основе сигнатур и правил // Искусственный интеллект и принятие решений. 2025. № 1. С. 3-13.
2. Snehi J., Bhandari A., Baggan V., Snehi M., Kaur H. AIDAAS: Incident handling and remediation anomaly-based IDaaS for cloud service providers // 2021 10th International Conference on System Modeling & Advancement in Research Trends (SMART). IEEE. 2021. P. 356-360.
3. Huang Z., Gu Y., Zhao Q. One-Class Directed Heterogeneous Graph Neural Network for Intrusion Detection // 2022 6th International Conference on Innovation in Artificial Intelligence (ICIAI). ACM. 2022. P. 178-184.
4. Maasaoui Z., Merzouki M., Battou A., Lbath A. Anomaly Based Intrusion Detection using Large Language Models // 2024 IEEE/ACS 21st International Conference on Computer Systems and Applications (AICCSA). IEEE. 2024. P. 1-8.
5. Farrukh Y. A., Wali S., Khan I., Bastian N. D. XG-NID: Dual-Modality Network Intrusion Detection using a Heterogeneous Graph Neural Network and Large Language Model // arXiv preprint arXiv:2408.16021. 2024. 19 p.
6. Kotenko I., Chechulin A., Novikova E. Attack Modelling and Security Evaluation for Security Information and Event Management // SECURE 2012 - Proceedings of the International Conference on Security and Cryptography. 2012. P.391-394.
7. Десницкий В.А., Чечулин А.А., Котенко И.В., Левшун Д.С., Коломеец М.В. Комбинированная методика проектирования защищенных встроженных устройств на примере системы охраны периметра // Труды СПИИРАН. 2016. № 5 (48). С. 5-31. DOI: 10.15622/sp.48.1.
8. Desnitsky V., Levshun D., Chechulin A., Kotenko I. Design technique for secure embedded devices: application for creation of integrated cyber-physical security system // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications. 2016. Vol.7. No.2. P.60-80. DOI: 10.22667/JOWUA.2016.06.31.060.

УДК 355.018.3:004.8:658.482

#### УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПОДРАЗДЕЛЕНИЯХ ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ В КОНТЕКСТЕ РАЗВИТИЯ И РАСПРОСТРАНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

**Афонин Петр Николаевич**

Академия войск национальной гвардии

Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия

e-mail: pnafonin@yandex.ru

**Аннотация.** В статье исследуются трансформация и усложнение ландшафта угроз информационной безопасности (ИБ) подразделений Росгвардии, обусловленные активным развитием и внедрением технологий искусственного интеллекта (ИИ). Анализируются новые классы рисков, связанные с использованием интеллектуальных автономных систем, алгоритмов машинного обучения и технологий генеративного ИИ потенциальными противниками. Обосновывается необходимость адаптации существующих систем управления рисками ИБ. Предлагаются ключевые направления развития методологии и практики управления рисками ИБ, включая создание специализированных систем мониторинга угроз на базе ИИ, разработку новых регламентов

тестирования и аттестации интеллектуальных систем, а также совершенствование подготовки специалистов в области ИБ.

**Ключевые слова:** управление рисками информационной безопасности; искусственный интеллект; машинное обучение; войска национальной гвардии; кибербезопасность; генеративный ИИ; автономные системы.

## INFORMATION SECURITY RISK MANAGEMENT IN NATIONAL GUARD UNITS IN THE CONTEXT OF THE DEVELOPMENT AND DISSEMINATION OF ARTIFICIAL INTELLIGENCE

Afonin Petr

Academy of the National Guard Troops  
1 Pilot Pilyutova St., St. Petersburg, 198206, Russia  
e-mail: pnafonin@yandex.ru

**Abstract.** The article examines the transformation and complication of the information security threat landscape of Rosgvardiya units due to the active development and implementation of artificial intelligence (AI) technologies. New classes of risks associated with the use of intelligent autonomous systems, machine learning algorithms, and generative AI technologies by potential adversaries are analyzed. The necessity of adapting existing information security risk management systems is substantiated. Key directions for the development of information security risk management methodology and practice are proposed, including the creation of specialized AI-based threat monitoring systems, the development of new regulations for testing and certifying intelligent systems, as well as improving the training of information security specialists.

**Keywords:** information security risk management; artificial intelligence; machine learning; National Guard troops; cybersecurity; generative AI; autonomous systems.

Войска национальной гвардии Российской Федерации (Росгвардия) как компонент сил обеспечения государственной безопасности выполняют критически важные задачи по защите конституционного строя, общественного порядка и противодействию терроризму и экстремизму [1]. Информатизация и цифровая трансформация процессов управления, разведки, связи и обеспечения неизбежно сопровождаются ростом зависимости от информационных систем и технологий [2]. Это, в свою очередь, расширяет поверхность для потенциальных атак и повышает значимость эффективного управления рисками информационной безопасности (ИБ).

Параллельно с этим наблюдается взрывной рост возможностей технологий искусственного интеллекта (ИИ). Если изначально ИИ рассматривался преимущественно как инструмент для усиления систем защиты, то сегодня очевидно, что он становится источником новых, качественно более сложных угроз. Противник, обладающий доступом к продвинутым ИИ-технологиям, способен проводить атаки с беспрецедентной скоростью, масштабом и адаптивностью [3]. В данной связи актуализируется задача фундаментального пересмотра существующих подходов к управлению рисками ИБ в подразделениях Росгвардии с учетом вызовов, порождаемых эрой ИИ.

Целью представляемой работы является анализ новых рисков ИБ, обусловленных развитием ИИ, и разработка предложений по модернизации системы управления этими рисками в подразделениях Росгвардии.

Проведенные исследования позволили определить, что новая парадигма угроз заключается в том, что риски ИБ порождаются технологиями ИИ [4]. Именно поэтому традиционные модели угроз ИБ, основывающиеся на действиях злоумышленника-человека или относительно статичных вредоносных программ, требует корректировки в части внесения следующих ключевые изменения:

1. Интеллектуализация кибератак. Системы ИИ позволяют автоматизировать не только разведку и сканирование уязвимостей, но и проведение целевых атак. Например, ИИ-алгоритмы могут:

- генерировать фишинговые сообщения и глубокие подделки (deepfakes) высочайшего качества для целенаправленного социального инжиниринга против командного состава;
- проводить высокоскоростные атаки методом перебора (brute-force), адаптируясь к системам обнаружения вторжений;
- создавать полиморфные и метаморфные вредоносные программы, способные изменять свой код для обхода сигнатурных систем защиты.

2. Угрозы для автономных систем и роботизированных комплексов. Росгвардия активно внедряет беспилотные летательные аппараты (БПЛА), автономные системы наблюдения и другие робототехнические комплексы. Риски заключаются в возможности перехвата управления, подавления каналов связи или внесения деструктивных команд в систему принятия решений такой платформы с помощью атак на ее алгоритмы ИИ [5].

3. Компрометация данных для обучения ИИ. Эффективность моделей ИИ напрямую зависит от качества и достоверности данных, на которых они обучены. Противник может осуществлять целенаправленное «отравление» (data poisoning) наборов данных, используемых для тренировки служебных систем ИИ (например, систем распознавания образов или анализа угроз). Это приведет к некорректной работе системы в критический момент.

4. Генеративный ИИ как инструмент создания синтетических угроз. Технологии генеративного ИИ (например, GPT, Stable Diffusion) позволяют создавать реалистичные, но полностью синтетические контент, голосовые сообщения и видео [6, 7]. Это создает риски дезинформации, провокаций и манипуляции личным составом и населением в зоне ответственности подразделений.

Указанные изменения требуют адаптации системы управления рисками ИБ к вызовам ИИ, при этом стандартный процесс управления рисками ИБ (идентификация, оценка, обработка, мониторинг) требует модернизации [8, 9].

Идентификация рисков. Необходимо расширить классификаторы угроз, включив в них специфические ИИ-риски:

- риск компрометации модели ИИ;
- риск «отравления» данных обучения;
- риск генерации синтетических медиа для дезинформации;
- риск атак на системы с элементами автономности.

Оценка рисков. Традиционные качественные и количественные методы оценки должны быть дополнены моделированием с использованием «красных команд» (red teaming), оснащенных собственными ИИ-инструментами для имитации атак продвинутого противника. Это позволит более адекватно оценить вероятность и воздействие новых угроз.

Обработка рисков. Ключевые направления:

- разработка и внедрение «ИИ-щита»: создание и развертывание собственных систем ИИ, предназначенных для противодействия ИИ-атакам. К таким системам относятся, в частности, системы обнаружения аномалий в реальном времени, инструменты для выявления deepfake-контента, системы мониторинга поведения автономных платформ;

- пересмотр и разработка нормативно-методического обеспечения, в части создания строгих регламентов и стандартов для проектирования, тестирования, сертификации и эксплуатации всех систем, использующих ИИ, в подразделениях Росгвардии. Особое внимание должно уделяться вопросам объяснимости и устойчивости алгоритмов.

- защита критически важных данных обуславливается тем, что происходит постоянное ужесточение политик управления данными, особенно теми, что используются для обучения моделей ИИ, что определяет необходимость применения методов дифференциальной приватности и шифрования данных на всех этапах их жизненного цикла;

- подготовка кадров: требуется внедрение в программы подготовки специалистов по ИБ в Академии Росгвардии и на курсах повышения квалификации дисциплин, связанных с основами ИИ, методами противодействия ИИ-угрозам и юридическими аспектами применения ИИ в силовых структурах;

- институциональное развитие: развитие научно-методических принципов противодействия угрозам, возникающим вследствие развития и распространения ИИ, требует создания на базе Академии Росгвардии специализированного подразделения научно-исследовательского института «Системного анализа проблем искусственного интеллекта в войсках национальной гвардии России».

Таким образом, развитие и распространение искусственного интеллекта носят двойственный характер для подразделений Росгвардии. С одной стороны, ИИ открывает колоссальные возможности для повышения эффективности выполнения задач. С другой стороны, он порождает новый класс высокоадаптивных и масштабируемых угроз информационной безопасности, борьба с которыми традиционными методами становится неэффективной.

Управление рисками ИБ в новых условиях требует проактивного, а не реактивного подхода. Необходима скоординированная работа по развитию нормативной базы, внедрению специализированных технических средств защиты на базе контринтеллектуальных систем и, что наиболее важно, непрерывной подготовке кадров, способных понимать, эксплуатировать и защищаться от технологий ИИ. Только комплексный подход, интегрирующий технологические, организационные и кадровые меры, позволит обеспечить необходимый уровень защищенности информационного пространства подразделений Росгвардии в условиях стремительной цифровой трансформации.

## СПИСОК ЛИТЕРАТУРЫ

1. Директива Росгвардии от 28 октября 2021 г. № Д-2 «О приоритетных направлениях деятельности войск национальной гвардии Российской Федерации в 2022 году» // Сайт Росгвардии. URL: <https://rosguard.gov.ru/> (дата обращения: 20.07.2025).
2. Доктрина информационной безопасности Российской Федерации // URL: <https://rg.ru/documents/2016/12/06/doktrina-infobezobasnost-site-dok.html> (дата обращения: 20.07.2025).
3. Стратегия развития искусственного интеллекта в Российской Федерации на период до 2030 года (утверждена Указом Президента РФ № 490 от 10.10.2019).
4. Подход к анализу военно-политической обстановки и прогнозированию военных угроз на основе ассоциативного анализа / П. Н. Афонин, А. Н. Проников, А. М. Сазыкин, П. А. Фалеев // Известия Российской академии ракетных и артиллерийских наук. 2025. № 1(136). С. 9-17. DOI 10.53816/20753608\_2025\_1\_9. EDN KVQRFU.
5. Афонин, П. Н. Управление стеком технологических инноваций в войсках национальной гвардии / П. Н. Афонин // Системный анализ и логистика. 2025. № 3(46). С. 66-71. DOI 10.31799/2077-5687-2025-3-66-71. EDN MOKMXS.
6. Афонин, П. Н. Применение искусственного интеллекта для анализа массива данных, формируемых с использованием интегрированной информационной системы пункта пропуска / П. Н. Афонин, А. Ю. Лебедева // Вестник Российской таможенной академии. 2024. № 1(66). С. 97-112. EDN YKSNWC.
7. Гнатик, Е. Н. Милитаризация систем искусственного интеллекта: возможности и угрозы / Е. Н. Гнатик // Вестник Российского университета дружбы народов. Серия: Философия. 2024. Т. 28, № 3. С. 771-784. DOI 10.22363/2313-2302-2024-28-3-771-784. EDN VZSWGK.
8. Кочарян, Г. С. Внедрение и перспективы ИИ в военно-управленческих системах / Г. С. Кочарян // Интеллектуальные ресурсы региональному развитию. 2025. № 1. С. 92-96. EDN FCAYUI.
9. Apruzzese G. et al. The Role of Machine Learning in Cybersecurity / G. Apruzzese, P. Laskov, E. Montes de Oca, W. Mallouli, L. Búrdalo, A. Grammatopoulos, F. Franco // Digital Threats: Research and Practice. 2023. Vol. 4, Issue 1. Pp. 812-832.



УДК 004.056.5

## ПРЕДПОСЫЛКИ И НАЗНАЧЕНИЕ МОДЕЛИ ПОВЕДЕНИЯ НЕУМЫШЛЕННОГО ИНСАЙДЕРА В ИНФОРМАЦИОННОЙ СИСТЕМЕ ОРГАНИЗАЦИИ

Буйневич Михаил Викторович<sup>1</sup>, Моисеенко Григорий Юрьевич<sup>2</sup>, Жернова Ксения Николаевна<sup>3</sup>

<sup>1</sup> Санкт-Петербургский университет ГПС МЧС России  
Московский пр., 149, Санкт-Петербург, 196105, Россия

<sup>2</sup> Министерство обороны Российской Федерации  
Знаменка ул., 19, Москва, 119160, Россия

<sup>3</sup> СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия  
e-mails: bmv1958@yandex.ru, mogreq@mail.ru, zhernova@comsec.spb.ru

**Аннотация.** Рассматриваются проблема неумышленного инсайдинга в организации, обосновывается необходимость создания модели его поведения, приводятся основные предпосылки к созданию, а также назначение модели с позиции информационной безопасности.

**Ключевые слова:** неумышленный инсайдинг; информационная система; модель поведения; девиативность; информационная безопасность.

## PREREQUISITES AND PURPOSE OF THE UNINTENTIONAL INSIDER BEHAVIOR MODEL IN THE ORGANIZATION'S INFORMATION SYSTEM

Buinevich Mikhail<sup>1</sup>, Moiseenko Grigory<sup>2</sup>, Zhernova Ksenia<sup>3</sup>

<sup>1</sup> St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia  
149 Moskovskiy Av, St. Petersburg, 196105, Russia

<sup>2</sup> Ministry of Defense of the Russian Federation  
19 Znamenka St, Moscow, 119160, Russia

<sup>3</sup> St. Petersburg Federal Research Center of the Russian Academy of Sciences  
39 14th Line VO, St. Petersburg, 199178, Russia

e-mails: bmv1958@yandex.ru, mogreq@mail.ru, zhernova@comsec.spb.ru

**Abstract.** The problem of unintentional insider in an organization is considered, the need to create a model of its behavior is substantiated, the main prerequisites for its creation are given, as well as the purpose of the model from the information security standpoint.

**Keywords:** unintentional insider; information system; behavior model; deviance; information security.

Обеспечение информационной безопасности (ИБ) является неотъемлемой частью деятельности любой организации. Сложность данного процесса обусловлена наличием внушительного количества источников атак, особое место среди которых занимают инсайдерские — иницируемые сотрудниками организации, уже находящимися внутри защищаемого периметра [1]. Задача противодействия им усложняется, если легальный сотрудник, выполняя должностные обязанности, становится нарушителем вследствие девиативного поведения, присущего любому человеку — возникает так называемый «неумышленный инсайдинг».

Помимо очевидных способов противодействия неумышленному инсайдингу, направленных на самих сотрудников, альтернативным и относящимся более к организационным может стать изначальное проектирование регламентов деятельности, которые устойчивы к поведению человека [2]. Для этого требуется создание соответствующей модели поведения сотрудника в информационной системе (ИС) организации, отражающей возможные нарушения им должностных инструкций.

Так, во-первых, выполнение инструкций представимо, как переходы между состояниями ИС, задаваемыми точками многомерного пространства их признаков [3].

Во-вторых, девиативность поведения сотрудника будет приводить к ошибочным переходам в состояния-точки, близкие к требуемым.

И, в-третьих, сами состояния могут иметь определенную иерархию, отражающую строение современных графических интерфейсов — группы элементов, графические формы и др.

Основное назначение модели — симуляция поведения «неумышленного инсайдера» и последующая оценка возможных нарушений ИБ минимум по трем сценариям «неумышленных» кибератак.

Во-первых, в случае перехода ИС в состояние, ведущее к существенно иной логике выполнения инструкции; процесс работы в ней сотрудника не будет завершен в принципе, что может трактоваться, как нарушение доступности (услуги).

Во-вторых, ввод сотрудником данных «не в то» поле хотя и может привести к получению услуги, но для некорректно заданной информации — нарушение целостности.

И, в-третьих, ввод конфиденциальных данных в поле, значение которого в процессе или после предоставления услуги заносится в открытое хранилище — нарушение конфиденциальности.

*Работа выполнена при поддержке гранта Российского научного фонда и Санкт-Петербургского научного фонда № 24-21-20058 (<https://rscf.ru/project/24-21-20058/>) в СПб ФИЦ РАН.*

## СПИСОК ЛИТЕРАТУРЫ

1. Буйневич М.В., Власов Д.С., Моисеенко Г.Ю. Комбинирование способов выявления инсайдеров больших информационных систем // Вопросы кибербезопасности. 2024. № 3 (61). С. 2-13. DOI: 10.21681/2311-3456-2024-3-2-13.
2. Буйневич М.В., Моисеенко Г.Ю. Повышение «устойчивости» регламентов деятельности как способ противодействия неумышленному инсайдингу // Вопросы кибербезопасности. 2024. № 6 (64). С. 108-116. DOI: 10.21681/2311-3456-2024-6-108-116.
3. Власов Д.С. К вопросу о признаках инсайдерской деятельности // Национальная безопасность и стратегическое планирование. 2024. № 1 (45). С. 35-45. DOI: 10.37468/2307-1400-2024-1-35-45.

УДК 004.056.5

**АНАЛИЗ АКТИВНОСТИ ПОЛЬЗОВАТЕЛЕЙ В СОЦИАЛЬНОЙ СЕТИ «ВКОНТАКТЕ»****Виткова Лидия Андреевна<sup>1</sup>, Лебедева Дарья Александровна<sup>2</sup>**<sup>1</sup> СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия

<sup>2</sup> Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Большевикова пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

e-mails: lidia.vitkova@yandex.ru, dashlele@yandex.ru

**Аннотация.** Представленное исследование посвящено всестороннему анализу активности пользователей в сообществе «ВКонтакте» с целью выявления структуры коммуникационного ядра и определения доли искусственно сгенерированной активности. В работе описывается методология категоризации пользователей на основе их вовлечённости (от «наблюдателя» до «лидера») и применяются алгоритмы на языке Python для сбора, обработки и анализа данных.

**Ключевые слова:** социальные сети; анализ активности; обнаружение искусственной активности; искусственная медиатизация; накрутка; репутационные риски информационной безопасности.

**USER ACTIVITY ANALYZING ON THE «VKONTAKTE» SOCIAL NETWORK****Vitkova Lidia<sup>1</sup>, Lebedeva Daria<sup>2</sup>**<sup>1</sup> St. Petersburg Federal Research Center of the Russian Academy of Sciences

39 14th Line VO, St. Petersburg, 199178, Russia

<sup>2</sup> The Bonch-Bruевич Saint Petersburg State University of Telecommunications

22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia

**Abstract.** The presented study is devoted to a comprehensive analysis of user activity in the VKontakte community in order to identify the structure of the communication core and determine the proportion of artificially generated activity. The paper describes a methodology for categorizing users based on their engagement (from «observer» to «leader») and uses Python algorithms to collect, process, and analyze data.

**Keywords:** social network analysis; user activity analysis; inducted activity detection.

В работе была поставлена цель исследования — оценка корректности методов СММ-продвижения страницы организации на примере официальной страницы компании в социальной сети «ВКонтакте» для сокращения возможных репутационных рисков. Для достижения цели был проведен анализ активности пользователей сообщества, выявлено коммуникативное ядро. Также был определена доля искусственно созданной активности. Для оценки аудитории сообщества использовалась методология, предложенная в [1]. В ходе исследования активности сообщества и пользователей были разработаны программные компоненты для сбора данных из социальной сети, предобработки и анализа. Алгоритмы реализованы на языке Python. Для удобства, данные и программы собраны в репозитории [2].

На первом этапе исследования была получена информация об активности сообщества в период с апреля 2020 по начало июля 2025 года, далее данные были размечены. На следующем этапе проводился анализ. Прежде всего было рассмотрено количество постов, просмотров и лайков за каждый месяц исследуемого периода. Анализ показал, что основная активность сообщества и аудитории приходится на 2023-2024 годы, в то время как в 2020-2021 годах активность сообщества была значительно ниже, чем в последующих. Активность пользователей в период с февраля по сентябрь 2023 резко возрастает. Распределение постов по количеству просмотров говорит о том, что основная масса постов имеет от 100 до 1000 просмотров. В рассматриваемой выборке посты, набравшие более 1000 просмотров, можно считать аномалией, так как их количество составляет менее 5 %.

Далее было изучено содержание [3] популярных постов. Определены 2 группы ключевых слов: относящиеся к розыгрышам и событиям. Подсчитано количество просмотров на постах, относящихся к данным тематикам. Среднее количество просмотров на таких постах — 2552,33. К данным группам относится около 4,3 % всех постов в сообществе.

Пользователи, которые проявляли активность (отметка мне нравится (лайк), комментарий) были разделены на классы в соответствии с методикой [1]. Среди пользователей, оставлявших оценки и комментарии на посты сообщества сделаны репрезентативные выборки, включающие в себя по 1000 строк. Анализ показал, что среди пользователей, оставлявших комментарии, «людей» — 12,34 %, «ботов» — 87,56 %, удаленных

страниц — 11,3 %. Среди пользователей, оставивших оценки, «людей» — 18,9 %, «ботов» — 81,1 %, удаленных страниц — 8,4 %.

В коммуникативное ядро [1] входит всего 5,31 % от количества пользователей, оставивших на странице сообщества хоть один комментарий. Среднее количество комментариев, оставляемых этими пользователями, составляет около 93 % от общей массы, что говорит о том, что данная группа по большей части влияет на показатель активности всего сообщества. Ядро по лайкам составляет 1,15 % от общего количества пользователей, хоть единожды поставивших на постах сообщества оценку. Среднее количество лайков, оставляемых этими пользователями, составляет 99 % от общей массы, что говорит о том, что данная группа составляет основную активность сообщества. Кроме того, коммуникативное ядро рассмотрено с точки зрения внешней к тематике аудитории. Собрана информация о том, кто из пользователей-людей является сотрудником организации, которой принадлежит сообщество. Показано, что сотрудники организации и «боты» занимают наиболее значительную часть аудитории сообщества. В данном исследовании под термином «бот» понимается «искусственно созданный профиль». Такие профили определялись путем оценки количества и качества подписок и репостов на странице [4].

На третьем этапе в ходе исследования была выдвинута гипотеза, что активность под наиболее популярными постами создана искусственно. В случае подтверждения гипотезы можно предположить, что обнаружение «искусственной медиатизации» («накрутки») компаниями конкурентами может нанести ущерб репутации компании.

Для проверки гипотезы были выбраны наиболее популярные посты и активность комментаторов под ними. Собраны посты, на которых есть как минимум 1 комментарий. По таблице с репрезентативной выборкой из 1000 пользователей, для которых определен статус бот/человек, рассмотрена активность под каждым постом. Получена таблица, в которой отражена информация об адресе в сети Интернет каждого поста (URL-адрес). Также в таблицу была добавлена информация о количестве комментариев к посту, отдельно выделено количеству комментариев от подтвержденных «людей» и «ботов». В целом, рассмотрев процентное соотношение людей/ботов по репрезентативной выборке, можно сказать, что на наиболее популярные посты активность в комментариях создана искусственно. Таким образом гипотеза подтверждается.

Сбор данных, предобработка, анализ поведился с учетом возможностей и ограничений социальной сети «ВКонтакте», следовательно, любое заинтересованное лицо может провести подобный анализ и обнаружить признаки искусственной медиатизации. При этом исследование показало, что аудитория сообщества на 80 % состоит из искусственно привлеченных страниц-ботов; коммуникативное ядро более чем на 70 % состоит из ботов и сотрудников организации; на посты, направленные на внешнюю аудиторию (мероприятия, конкурсы, события), активность создается искусственно.

#### СПИСОК ЛИТЕРАТУРЫ

1. Gavra D. et all. Detection of Induced Activity in Social Networks: Model and Methodology. Future Internet. 2021; 13(11):297. (Журнал, Q2, SCOPUS, WoS)
2. Ashley Smith. Social Network Bots Analysis [Электронный ресурс] // Github. 2025. URL: <https://github.com/loony-ash/social-network-bots> (дата обращения 20.08.2025)
3. Стилметрия, или как отличить Акунина от Булгакова с помощью 50 строк кода? [Электронный ресурс] // Habr. 2021. URL: <https://habr.com/ru/articles/536858/> (дата обращения 02.08.2025)
4. Ботнадзор: Выявляем ботов в VK // Ботнадзор. URL: <https://botnadzor.org/> (дата обращения: 10.08.2025).

УДК 004.056.5

#### МЕТА-МОДЕЛЬ СОТРУДНИКА ОРГАНИЗАЦИИ ДЛЯ ВЫЯВЛЕНИЯ ИНСАЙДЕРСКОЙ ДЕЯТЕЛЬНОСТИ

**Власов Дмитрий Сергеевич<sup>1</sup>, Мелешко Алексей Викторович<sup>2</sup>**

<sup>1</sup> Главное управление МЧС России по г. Санкт-Петербургу

наб. реки Мойки, д. 85, Санкт-Петербург, 190000, Россия

<sup>2</sup> СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия

e-mails: prikerx@bk.ru, meleshko.a@iiias.spb.su

**Аннотация.** Одной из существенных угроз информационной безопасности любой организации является наличие инсайдеров, которые способны осуществлять атаки изнутри ее периметра. Для их эффективного выявления требуется соответствующая модель, обобщенная структура которой может представлять собой совокупность частных, отражающих в первую очередь различные аспекты самого человека, а не его поведения.

**Ключевые слова:** информационная безопасность; инсайдер; выявление; модель; сетевые соединения.

#### META-MODEL OF AN ORGANIZATIONAL EMPLOYEE FOR DETECTING INSIDER ACTIVITY

**Vlasov Dmitry<sup>1</sup>, Meleshko Alexey<sup>2</sup>**

<sup>1</sup> Main Directorate of the Ministry of Emergency Situations in the city of St. Petersburg

85 Moika River Emb., St. Petersburg, 190000, Russia

<sup>2</sup> Saint-Petersburg Federal Research Center of the Russian Academy of Sciences

39 14th Line VO, St. Petersburg, 199178, Russia

e-mails: prikerx@bk.ru, meleshko.a@iiias.spb.su

**Abstract.** One of the significant information security threats of any organization is the presence of insiders who are capable of carrying out attacks from within its perimeter. To effectively identify them, a corresponding model is required, the generalized structure of which can be a set of private ones, reflecting primarily various aspects of the person himself, and not his behavior.

**Keywords:** information security; insider; detection; model; network connections.

Наличие инсайдера является существенной проблемой для информационной безопасности организации, поскольку он в отличие от внешних нарушителей априори обладает большими возможностями для проведения атак. Проблема усложняется тем, что внутренний нарушитель может скрывать как свои мотивы, так и злонамеренные действия, делая задачу его обнаружения еще более сложной. Поэтому требуется применение целого комплекса методов, которые должны быть объединены в единый — мета-метод.

Поскольку для работы методов обнаружения инсайдеров, как правило, требуется соответствующая модель [1], то аналогичным образом должен строиться и мета-метод. А исходя из гетерогенности признаков сотрудника-инсайдера (техническая подготовленность, психологическая устойчивость, финансовые и иные жизненные трудности, поведение в сети организации, собираемые данные и пр.), его модель должна связывать всех их ожидаемо сложным образом.

Для этого можно построить частные модели, связанные с отдельными, специфичными для него, проявлениями сотрудника, объединяемые затем в более общую. Например, установление сетевых соединений с информационным ресурсом организации и физическое посещение сотрудником принципиально новых помещений может описываться одной частью модели, связанной с его поведением относительно должностных инструкций; при этом, дополнительно может учитываться и ответственность сотрудника к выполнению своих обязанностей.

Таким образом, одним из первых шагов к созданию мета-метода выявления инсайдера в организации, является создание мета-модели, объединяющей частные модели, каждая из которых учитывает собственный аспект поведения сотрудника. И хотя вопрос выделения частных моделей требует отдельного исследования, но уже сейчас можно предположить следующие составные элементы. Во-первых, это модель компетенции — она должна описывать профессиональные навыки сотрудника, связанные в том числе, и с его опытом (как текущим, так и на предыдущем месте работы). Во-вторых, модель мотивации — должна отражать его стремление к достижению целей, коррелирующих (но потенциально и противоположных) с существующими в организации. В-третьих, модель личности — должна характеризовать сотрудника с позиции человеческих факторов, таких, как доверчивость, обидчивость, любознательность и пр. В-четвертых, модель социальных взаимоотношений — должна определять как степень его взаимодействия с окружающими людьми, так и способность распознавать чужие эмоции и мотивации. И, в-пятых, модель потенциала — должна учитывать возможности сотрудника к саморазвитию. Каждая из перечисленных моделей, с одной стороны, является внутренней для сотрудника, а с другой — связана с его внешними проявлениями, которые могут служить признаками инсайдерской деятельности (например, в виде аномалий [2, 3]); при этом, все модели объединены в одну, которая гипотетически способна давать более качественную оценку состояния сотрудника — например, от абсолютно лояльного, через неудовлетворенного и «на грани срыва» до полноценного нарушителя.

#### СПИСОК ЛИТЕРАТУРЫ

1. Власов Д.С. Мультикритериальная модель систематизации способов обнаружения инсайдера // Вопросы кибербезопасности. 2024. № 2 (60). С. 66-73. DOI: 10.21681/2311-3456-2024-2-66-73
2. Мелешко А.В., Шулепов А.А., Десницкий В.А., Новикова Е.С. Комбинированный подход к выявлению аномалий в беспроводных сенсорных сетях на примере системы управления водоснабжением // Компьютерные инструменты в образовании. 2021. № 1. С. 58-67. DOI: 10.32603/2071-2340-2021-1-59-68
3. Методы обнаружения инсайдерских признаков в больших данных [Электронный ресурс] // APNI. URL: <https://apni.ru/article/12167-metody-obnaruzheniya-insajderskih-priznakov-v-bolshih-dannyh> (дата обращения: 20.08.2025).

УДК 004.056.5

#### МОДЕЛИ АТАК, СЛЕДОВ И СРЕДЫ СОВЕРШЕНИЯ ИНЦИДЕНТОВ С ИСПОЛЬЗОВАНИЕМ АППАРАТА НЕЧЁТКОЙ ЛОГИКИ

Горда Максим Дмитриевич, Чечулин Андрей Алексеевич

СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия

e-mails: [gordamd@ya.ru](mailto:gordamd@ya.ru), [andreych@bk.ru](mailto:andreych@bk.ru)

**Аннотация.** Предложенный подход позволяет учитывать неполные и гетерогенные данные, систематизировать характеристики нарушителя, объекта воздействия и цифровых артефактов. Использование лингвистических и нечётких переменных обеспечивает возможность построения правил вывода и формирование обоснованных гипотез при расследовании. Разработанные модели повышают достоверность аналитических выводов и качество расследования инцидентов.

**Ключевые слова:** информационная безопасность; расследование инцидентов ИБ; объект воздействия; цифровые артефакты; модель атак.

## MODELS OF ATTACKS, TRACES, AND INCIDENT ENVIRONMENTS USING FUZZY LOGIC

Gorda Maxim, Chechulin Andrey

St. Petersburg Federal Research Center of the Russian Academy of Sciences

39 14th Line VO, St. Petersburg, 199178, Russia

e-mails: gordamd@ya.ru, andreych@bk.ru

**Abstract.** The proposed approach allows for the consideration of incomplete and heterogeneous data, as well as the systematization of the characteristics of the perpetrator, the object of influence, and digital artifacts. The use of linguistic and fuzzy variables enables the construction of inference rules and the formation of reasonable hypotheses during investigations. The developed models enhance the accuracy of analytical conclusions and the quality of incident investigations.

**Keywords:** information security; investigation of information security incidents; object of influence; digital artifacts; attack model.

Современные исследования показывают [1-3], что действующие подходы к расследованию инцидентов информационной безопасности имеют серьёзные ограничения. Цифровые следы зачастую являются неполными, скрытыми и не всегда пригодны для анализа. Методики устаревают, уровень подготовки специалистов остаётся недостаточным, а развитие технологий опережает теоретические и научные решения. Это подтверждает необходимость формализации процесса расследования и построения моделей, позволяющих учитывать неопределённость исходных данных и возможность их анализа на различных этапах расследования.

Расследование инцидента включает взаимосвязанные этапы. На этапе уведомления фиксируется факт потенциального инцидента. Затем проводится сбор информации и фиксация массивов данных с обеспечением их целостности. На стадии извлечения доказательств выделяются характеристики нарушителя и его методов, после чего осуществляется анализ и построение временных цепочек событий. Заключительный этап связан с представлением доказательств, визуализацией результатов и оценкой ущерба.

Для повышения эффективности расследования предложены формализованные модели среды, атак и цифровых следов с использованием аппарата нечёткой логики.

Модель среды инцидента включает:

- (1) нарушителя — тип субъекта (человек, автоматизированное или неавтоматизированное ПО), уровень квалификации (низкий, средний, высокий), методы (простые, умеренные, сложные);
- (2) объект воздействия — человек, программное или аппаратное обеспечение, операционная система. Основной параметр — уровень критичности (некритичный, умеренный, критичный);
- (3) взаимодействие — событие, в котором нарушитель воздействует на объект прямыми или косвенными методами.

Модель атак описывает:

- уровень опасности (неопасный, умеренно опасный, критический),
- результат (нарушение конфиденциальности, целостности, доступности),
- ущерб (незначительный, средний, серьёзный),
- уровень угрозы (низкий, средний, высокий).

Модель следов формализует цифровые артефакты через их качество (отсутствуют, недостаточные, достаточные), достоверность (сомнительная, частично достоверная, надёжная) и подозрительность действий (низкая, умеренная, высокая).

Все переменные задаются в виде лингвистических и нечётких, что позволяет учитывать неполные данные и плавные переходы значений. На их основе формируются правила вывода: ЕСЛИ объект критичный и методы сложные, ТО угроза высокая; ЕСЛИ следы достаточные и достоверные, ТО гипотеза подтверждается.

Таким образом, предложенные модели позволяют структурировать характеристики среды, атак и следов, формировать обоснованные гипотезы и работать в условиях неопределённости. Использование аппарата нечёткой логики повышает достоверность выводов и качество расследования инцидентов информационной безопасности.

*Работа выполнена при поддержке гранта Российского научного фонда и Санкт-Петербургского научного фонда № 25-11-20028 (<https://rscf.ru/project/25-11-20028/>) в СПб ФИЦ РАН.*

## СПИСОК ЛИТЕРАТУРЫ

1. Чечулин А.А., Горда М.Д., Котов А.А. Ключевые аспекты разработки междисциплинарной методики для внутренних расследований киберпреступлений // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2024. № 3. С. 70–85. DOI: 10.61260/2218-130X-2024-3-70-85.
2. Горда М. Д. Концепт ассистента для расследования инцидентов информационной безопасности на основе искусственного интеллекта / М. Д. Горда // Информатизация и связь. 2025. № 1. С. 123-128. DOI 10.34219/2078-8320-2025-16-1-123-128.
3. Горда М. Д., Чечулин А.А. Модель расследования киберпреступлений // Информатизация и связь. 2023. № 3. С. 92-97. DOI: 10.34219/2078-8320-2023-14-3-92-97.

УДК 004

**ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ПОВЫШЕНИЯ  
ЭФФЕКТИВНОСТИ УПРАВЛЕНИЯ ПРЕДПРИЯТИЕМ****Грачев Михаил Иванович**

Санкт-Петербургский университет МВД России  
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия  
e-mail: mig2500@mail.ru

**Аннотация.** В условиях роста киберугроз и цифровизации управленческих процессов обеспечение информационной безопасности (ИБ) становится критическим фактором эффективности предприятий. Предложена модель получения характеристик ИБ (технических, кадровых, финансовых) для достижения целевых показателей управленческой эффективности. Доказано, что решение обратной задачи распределения ресурсов на основе анализа состояний системы позволяет получать требуемые характеристики для гарантированного поддержания штатного функционирования организации при минимизации рисков.

**Ключевые слова:** информационная безопасность; эффективность управления; оптимизация ресурсов; киберугрозы; человеческий фактор; программно-аппаратный комплекс.

**ENSURING INFORMATION SECURITY TO IMPROVE ENTERPRISE MANAGEMENT EFFICIENCY****Grachev Mikhail**

St. Petersburg University of the Ministry of Internal Affairs of Russia  
1 Pilot Pilyutova St, St. Petersburg, 198206, Russia  
e-mail: mig2500@mail.ru

**Abstract.** In the context of growing cyber threats and digitalization of management processes, information security (IS) becomes a critical factor for enterprise efficiency. A model for optimizing IS resources (technical, personnel, financial) to achieve target management indicators is proposed. Solving the inverse problem of resource allocation based on system state analysis ensures guaranteed maintenance of normal operations while minimizing risks.

**Keywords:** information security; management efficiency; resource optimization; cyber threats; human factor; hardware/software complex.

В современных условиях усиления киберугроз [1] и технологического суверенитета обеспечение информационной безопасности предприятия требует комплексного подхода, интегрирующего технические, кадровые и управленческие аспекты. Ключевой проблемой является неэффективность прямого внедрения ресурсов ИБ без оптимизации их взаимодействия [2].

Предлагаемая модель основана на анализе состояний системы управления: штатная работа (целевое состояние); идентификация угрозы (требует квалифицированного персонала [3]); нейтрализация угрозы (зависит от технического оснащения [4]); совместная обработка инцидента (координация ресурсов).

Ключевой показатель эффективности — вероятность поддержания штатного режима (P00), достигается решением обратной задачи: определением оптимального сочетания ресурсов ИБ для заданного уровня защищенности. Ресурсная оптимизация включает:

- Технические средства (отечественные ПАК, шифрование каналов [5]), влияющие на скорость нейтрализации угроз.

- Квалификацию персонала (регулярная переподготовка [6]), определяющую точность идентификации инцидентов.

- Финансовое обеспечение для масштабирования ресурсов.

- Имитационное моделирование [7] для прогнозирования эффективности решений.

Практические рекомендации:

- приоритет отечественных ИТ-решений;

- обязательное шифрование данных;

- системное обучение сотрудников ИБ;

- динамическое перераспределение ресурсов на основе мониторинга состояний системы.

Комплексное управление ресурсами ИБ через решение обратной задачи обеспечивает устойчивость предприятия к угрозам при достижении целевых показателей эффективности управления.

**СПИСОК ЛИТЕРАТУРЫ**

1. Интерактивная карта киберугроз Kaspersky: [Электронный ресурс]. <https://cybermap.kaspersky.com/ru>
2. Трошин, Д. В. Безопасность предприятия: смысл, онтология, оценка / Д. В. Трошин. Тверь: ТвГУ, 2015. 212 с.
3. Скворцов, И. П. О проблеме человеческого фактора в обеспечении информационной безопасности / И. П. Скворцов, А. О. Титарев // Воздушно-космические силы. Теория и практика. 2022. № 23. С. 106-113.
4. Золотова, В. А. Направления развития интеллектуальной информационной технологии прогнозирования состояния предприятий промышленности России в условиях неблагоприятных внешних воздействий / В. А. Золотова 2022. № 4(86). С. 71-78.
5. Грачев, М. И. Математическая модель для принятия решений по противодействию киберугрозам в производстве / М. И. Грачев, В. Г. Бурлов // Информационные технологии в проектировании и производстве. 2022. № 4(188). С. 22-27.
6. Бурлов, В. Г. О необходимости подготовки и переподготовки кадров в сфере безопасности информационных технологий / В. Г. Бурлов, М. И. Грачев, А. И. Примакин // ИБРР-2017. СПб., 2017. С. 470-472.
7. Грачев, М. И. Имитационное моделирование процессов управления / М. И. Грачев // Интеллектуальные системы в производстве. 2022. Т. 20, № 4. С. 64-71.

УДК 004.056

**ИСПОЛЬЗОВАНИЕ ИИ ДЛЯ АНАЛИЗА SBOM И ТРИАЖА УЯЗВИМОСТЕЙ В ОТКРЫТОМ ПО  
Давыдов Виталий Владимирович<sup>1</sup>, Козырев Владислав Сергеевич<sup>2</sup>**<sup>1,2</sup> Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевиков пр., 22, к. 1, Санкт-Петербург, 193232, Россия<sup>1</sup> ООО «Газинформсервис»

Кронштадтская ул., 10, лит. А, Санкт-Петербург, 198096, Россия

<sup>2</sup> ООО «Р-Вижн»

Энтузиастов б-р, 2, эт. 23, Москва, 109544, Россия

e-mails: cjdjd66@gmail.com, vhlebokazov@gmail.com

**Аннотация.** В работе рассматривается практический подход к приоритизации уязвимостей в открытом программном обеспечении на основе перечня составных компонентов программного обеспечения. Предложен конвейер, который начинается с формирования и нормализации перечня, затем выполняется сопоставление уязвимостей, после этого проводится приоритизация, а завершающим этапом является подготовка заявлений в формате обмена сведениями об эксплуатируемости уязвимостей. Методы искусственного интеллекта применяются для аналитической оценки и классификационного ранжирования: нормализуются разнородные описания из реестра общих уязвимостей и экспозиций, из бюллетеней безопасности GitHub и из реестра уязвимостей открытого исходного кода, формируются краткие обоснования «затрагивает» либо «не затрагивает», подготавливаются рекомендации по устранению и черновые заявления указанного формата. Приоритизация учитывает совокупные сигналы — базовую оценку по Общей системе оценки уязвимостей версии 4.0, прогноз вероятности эксплуатации по системе прогнозирования эксплуатации уязвимостей, наличие записи в каталоге известных эксплуатируемых уязвимостей, область применения зависимости в производственной среде или среде разработки и достижимость уязвимого кода в конкретной сборке. Показана интеграция в конвейер непрерывной интеграции и поставки программного обеспечения с лёгким профилем на этапе до слияния изменений и полным профилем по расписанию, что снижает долю ложноположительных срабатываний и время аналитической обработки без замедления выпусков.

**Ключевые слова:** открытое программное обеспечение; SBOM; SCA; OSV; EPSS; KEV; CVSS; VEX; LLM; DevSecOps.

**AI-ASSISTED SBOM ANALYSIS AND VULNERABILITY TRIAGE IN OPEN-SOURCE SOFTWARE  
Davydov Vitaly<sup>1</sup>, Kozyrev Vladislav<sup>2</sup>**<sup>1,2</sup> Saint Petersburg State University of Telecommunications named after Prof. M. A. Bonch-Bruевич  
22 Bolshhevikov Av, St. Petersburg, 193232, Russia<sup>1</sup> ООО «Газинформсервис»

10 Kronshtadtskaya St., lit. A, St. Petersburg, 198096, Russia

<sup>2</sup> ООО «R-Vision»

2 Entuziastov B-d, fl. 23, Moscow, 109544, Russia

e-mails: cjdjd66@gmail.com, vhlebokazov@gmail.com

**Abstract.** The paper discusses a practical approach to prioritising vulnerabilities in open source software based on a list of software components. A pipeline is proposed that begins with the formation and normalisation of the list, followed by the comparison of vulnerabilities, then prioritisation, and finally the preparation of statements in the format of vulnerability exploitability information exchange. Artificial intelligence methods are used for analytical assessment and classification ranking: heterogeneous descriptions from the common vulnerability and exposure registry, GitHub security bulletins, and the open source vulnerability registry are normalised, brief justifications of ‘affected’ or ‘not affected’ are formed, recommendations for remediation and draft statements in the specified format are prepared. Prioritisation takes into account aggregate signals - the baseline assessment according to the Common Vulnerability Scoring System version 4.0, the exploitation probability forecast according to the vulnerability exploitation prediction system, the presence of an entry in the catalogue of known exploited vulnerabilities, the scope of application of the dependency in the production or development environment, and the accessibility of the vulnerable code in a specific build. Integration into the continuous integration and delivery pipeline is shown with a light profile at the pre-merge stage and a full profile on schedule, which reduces the false positive rate and analytical processing time without slowing down releases.

**Keywords:** open source software; SBOM; SCA; OSV; EPSS; KEV; CVSS; VEX; LLM; DevSecOps.

Современные практики безопасной разработки и эксплуатации программного обеспечения широко используют открытые пакеты, а программные продукты описываются через спецификации перечней составных компонентов программного обеспечения по стандарту обмена данными о программных пакетах, сокращённо стандарт SPDX, и по спецификации CycloneDX проекта OWASP [1–3]. Однако одного перечисления составных частей недостаточно для принятия решений - необходимо быстро определить, какие уязвимости действительно значимы в данном контексте.

Предлагаемый конвейер начинается с нормализации перечня составных компонентов и унификации идентификаторов пакетов, то есть унифицированных адресов пакетов url.

Далее выполняется сопоставление уязвимостей по реестру уязвимостей открытого исходного кода OSV с выравниванием соответствующих идентификаторов из регистра общих уязвимостей и экспозиций CVE, из бюллетеней безопасности GitHub GHSA и из идентификаторов записей реестра OSV.

На этапе приоритизации объединяются базовая оценка тяжести по Общей системе оценки уязвимостей версии 4.0, то есть методике CVSS версии 4.0, прогноз вероятности эксплуатации по Системе прогнозирования эксплуатации уязвимостей EPSS, наличие подтверждённой эксплуатации по Каталогу известных эксплуатируемых уязвимостей KEV, а также область применения зависимости и достижимость уязвимого кода. Итогом является прозрачный приоритет, применяемый в политиках блокировки релизов и при формировании задач [4–6].

Роль методов искусственного интеллекта — ускорение и повышение объяснимости. Большая языковая модель работает в изолированном режиме генерации с дополнением извлечёнными данными, обобщает разнородные бюллетени, формирует краткие резюме и обоснования «затрагивает» либо «не затрагивает», предлагает минимально рискованное обновление либо конфигурационные смягчения и готовит черновики заявлений в формате обмена сведениями об эксплуатируемости уязвимостей VEX для экспертной проверки. Все выводы сопровождаются ссылками на источники, включены контроль версий используемой модели и аудит формулировок запросов [7].

Интеграция проектируется двухпрофильной.

Лёгкий профиль на этапе до слияния изменений выполняет сопоставление и проверяет политики, например, при наличии признака в каталоге известных эксплуатируемых уязвимостей для зависимости, используемой в производственной среде.

Полный профиль запускается в ночные ежедневные и в еженедельные окна и дополняется анализом достижимости, выпуском артефактов - обновлённого перечня составных компонентов программного обеспечения, файлов в формате VEX и сводного отчёта.

Метрики эффективности включают снижение доли ложноположительных срабатываний, сокращение времени аналитической обработки на одну уязвимость в минутах и долю корректных пометок «не затрагивает» в документах VEX [8, 9]. Ограничения связаны с качеством внешних баз знаний, они компенсируются сопоставлением по нескольким источникам и использованием модели прогнозирования эксплуатации уязвимостей и каталога известных эксплуатируемых уязвимостей для приоритизации.

Таким образом, объединение перечня составных компонентов программного обеспечения, сигналов Системы прогнозирования эксплуатации уязвимостей и Каталога известных эксплуатируемых уязвимостей и методики Общей системы оценки уязвимостей, а также процедуры приоритизации и классификационной оценки с использованием больших языковых моделей систематизирует принятие решений и повышает эффективность безопасной разработки без существенного влияния на скорость релизов.

#### СПИСОК ЛИТЕРАТУРЫ

1. CycloneDX Specification. Version 1.6 [Электронный ресурс] / OWASP Foundation. URL: <https://cyclonedx.org> (дата обращения: 22.08.2025).
2. SPDX® Specification. Version 3.0 [Электронный ресурс] / SPDX Workgroup. URL: <https://spdx.dev> (дата обращения: 22.08.2025).
3. Open Source Vulnerabilities (OSV) — API и схема [Электронный ресурс]. URL: <https://osv.dev> (дата обращения: 22.08.2025).
4. Банк данных угроз безопасности информации (БДУ) [Электронный ресурс] / ФСТЭК России. URL: <https://bdu.fstec.ru> (дата обращения: 22.08.2025).
5. Запуск сканера в режиме SBOM [Электронный ресурс] / Лаборатория Касперского. 04.12.2024. URL: <https://support.kaspersky.ru/help/KCS/1.2/ru-RU/264539.htm> (дата обращения: 22.08.2025).
6. Инструкция по SCA: генерация SBOM, инструменты и практики [Электронный ресурс] / Habr, Swordfish Security. 05.03.2024. URL: [https://habr.com/ru/companies/swordfish\\_security/articles/797801/](https://habr.com/ru/companies/swordfish_security/articles/797801/) (дата обращения: 22.08.2025).
7. Что такое Software Bill of Materials и зачем он нужен [Электронный ресурс] / Habr. 19.12.2023. URL: <https://habr.com/ru/companies/mws/articles/781602/> (дата обращения: 22.08.2025).
8. SBOM (Software Bill of Materials): что это такое, функции и применение [Электронный ресурс] / Ростелеком-Солар. 17.02.2025. URL: [https://rt-solar.ru/products/solar\\_appscreener/blog/5251/](https://rt-solar.ru/products/solar_appscreener/blog/5251/) (дата обращения: 22.08.2025).
9. SBOM — русскоязычная страница проекта AlmaLinux [Электронный ресурс] / AlmaLinux OS Foundation. URL: <https://almalinux.org/ru/sbom/> (дата обращения: 22.08.2025).

УДК 004.056

#### РАЗРАБОТКА ЗАЩИЩЕННОГО ПРОТОКОЛА ДЕЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ В БЕСПРОВОДНОЙ СЕНСОРНОЙ СЕТИ

Десницкий Василий Алексеевич

СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия

e-mail: [desnitsky@comsec.spb.ru](mailto:desnitsky@comsec.spb.ru)

**Аннотация.** В работе предложен коммуникационный протокол децентрализованного управления в беспроводной сенсорной сети, предназначенный для организации защищенного обмена данными в сетях такого вида.

**Ключевые слова:** беспроводная сенсорная сеть; безопасность; протокол; децентрализация; самоорганизация; атака; моделирование; анализ.



## DEVELOPMENT OF SECURE PROTOCOL FOR DECENTRALIZED MANAGEMENT IN WIRELESS SENSOR NETWORKS

Desnitsky Vasily

St. Petersburg Federal Research Center of the Russian Academy of Sciences

39 14th Line VO, St. Petersburg, 199178, Russia

e-mail: desnitsky@comsec.spb.ru

**Abstract.** The study proposes a communication protocol for decentralized control in a wireless sensor network, designed for secure data exchange in wireless sensor networks.

**Keywords:** wireless sensor network; security; protocol; decentralization; self-organization; attack; modeling; analysis.

Предложенный в работе защищенный коммуникационный протокол децентрализованного управления в беспроводных сенсорных сетях (БСС) ориентирован на организацию безопасного взаимодействия узлов сети и обмена данными в условиях динамически изменяемых состава сети, ее структуры и функций мониторинга, возлагаемых на узлы БСС в процессе функционирования.

Протокол базируется на графовой модели БСС и модели атакующих воздействий, построенной на примере фрагмента беспроводной сенсорной сети соединенных беспилотных летательных аппаратов (БПЛА).

Протокол обеспечивает осуществление функций обнаружения атак на выделенном наборе узлов БСС с использованием расширенного набора информационных признаков, в том числе, признаков, характеризующих события отключения и подключения узлов к сети, изменения их местоположения в пространстве, изменения маршрутов доставки сообщений и прикладных событий мониторинга информационной безопасности [1]. Обнаружение атак осуществляется с использованием методов машинного обучения с учителем.

Коммуникационный протокол способствует выявлению атак сетевого уровня, направленных на нарушение процессов маршрутизации БСС и корректной идентификации узлов, таких как wormhole-атак, sinkhole-атак, а также Sybil-атак и др. [2].

Протокол специфицируется с использованием диаграмм последовательности, описывающих процедуры установления многосторонней сессии, в том числе обмена ключами, процедуры двустороннего и многостороннего обмена данными, процедуры присоединения и отсоединения узлов и процедуру корректного завершения текущей сессии.

К отличительным особенностям разработанного коммуникационного протокола можно отнести, во-первых, учет механизма децентрализованного управления в БСС на основе ролей узлов, при помощи которых организуются функции мониторинга информационной безопасности БСС [3].

При этом к реализуемым ролям узлов беспроводной БСС относятся роли сборщика данных, коллектора данных, хранителя данных и роль анализатора данных, в рамках которой осуществляются, в том числе, процессы детекторования атакующих воздействий и различного вида аномалий, происходящих в БСС.

Выполнимость и корректность протокола подтверждается путем тестирования с использованием имитационной модели БСС, построенный на основе правил функционирования узлов с каждой ролью и ориентированной на решение задач физического мониторинга инфраструктурных объектов с использованием БПЛА. Обоснованность модели и уровень защищенности обуславливается также учетом наиболее существенных видов атак на БСС, которые могут выполняться потенциальным атакующим, эксплуатирующим свойства самоорганизации и децентрализации сети.

*Исследование выполнено за счет гранта Российского научного фонда № 24-21-00486, <https://rscf.ru/project/24-21-00486/>.*

### СПИСОК ЛИТЕРАТУРЫ

1. Desnitsky V., Kotenko I., Rudavin N. Modeling and evaluation of battery depletion attacks on unmanned aerial vehicles in crisis management systems // Studies in Computational Intelligence. 2020. Т. 868. С. 323-332.
2. Oztoprak A., Hassanpour R., Ozkan A., Oztoprak K. Security Challenges, Mitigation Strategies, and Future Trends in Wireless Sensor Networks // A Review. ACM Comput. Surv. 2024. Vol. 57. No. 4, Article 104.
3. Desnitsky V., Kotenko I. Automated design, verification and testing of secure systems with embedded devices based on elicitation of expert knowledge // Journal of Ambient Intelligence and Humanized Computing. 2016. Т. 7. № 5. С. 705-719.

УДК 004.056

## ОЦЕНКА ИССЛЕДОВАТЕЛЬСКОГО ПРОТОТИПА САМООРГАНИЗУЮЩЕЙСЯ ДЕЦЕНТРАЛИЗОВАННОЙ БЕСПРОВОДНОЙ СЕНСОРНОЙ СЕТИ

Десницкий Василий Алексеевич

СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия

e-mail: desnitsky@comsec.spb.ru

**Аннотация.** В работе предложена и апробирована методика аналитической и экспериментальной оценки разрабатываемого прототипа самоорганизующейся децентрализованной беспроводной сенсорной сети в целях решения

задач моделирования и анализа процессов киберфизической безопасности. В рамках методики используются беспроводные коммуникационные интерфейсы XBee серии 2, одноплатные компьютеры Raspberry Pi и микроконтроллеры Arduino. Применяются методы моделирования, системного анализа, прототипирования и тестирования информационно-телекоммуникационных систем и сетей.

**Ключевые слова:** беспроводная сенсорная сеть; безопасность; децентрализация; самоорганизация; атака; оценка; моделирование.

## EVALUATION OF A RESEARCH PROTOTYPE OF A SELF-ORGANIZING DECENTRALIZED WIRELESS SENSOR NETWORK

Desnitsky Vasily

St. Petersburg Federal Research Center of the Russian Academy of Sciences

39 14th Line VO, St. Petersburg, 199178, Russia

e-mail: desnitsky@comsec.spb.ru

**Abstract.** The study presents and implements a technique for analytical and experimental evaluation of the developed prototype of a self-organizing decentralized wireless sensor network in order to solve problems of modeling and analysis of cyber-physical security processes. The technique relies on wireless communication interfaces XBee series 2, single-board computers Raspberry Pi and microcontrollers Arduino. Methods of modeling, system analysis, prototyping and testing of information systems and networks are used.

**Keywords:** wireless sensor network; security; decentralization; self-organization; attack; evaluation; modeling.

В рамках представляемого исследования проводится аналитическая и экспериментальная оценка разрабатываемого программно-аппаратного прототипа системы мониторинга киберфизической безопасности инфраструктурных объектов, таких как трубопроводы, промышленные предприятия, станции водоочистки и водоподготовки, с использованием технологий беспроводных сенсорных сетей (БСС), беспилотных летательных аппаратов и машинного обучения [1].

Лежащая в основе реализация БСС использует

- беспроводные коммуникационные интерфейсы XBee серии 2 — в качестве средств для динамически организуемой коммуникации в БСС;
- одноплатные компьютеры Raspberry Pi — в качестве основы для узлов с ролью анализатора данных и детектора;
- микроконтроллеры Arduino — для реализации узлов с ролями сборщика, обработчика и хранителя данных.

В рамках аналитической оценки производится анализ возможностей по реализации функций мониторинга физической безопасности с использованием динамических перестроений сети в процессе функционирования, а также возможностей динамического распределения и перераспределения ролей узлов, выполняющих функции сбора, предобработки, нормализации и агрегации первичных данных от сенсоров, пользовательских команд, а также прикладных и системных событий в БСС [2].

Тестирование работоспособности прототипа проводится на примере модели сети, состоящего из 4 узлов, где один из узлов монтируется непосредственно на корпус беспилотного летательного аппарата Parrot Bebop Drone 2.

Кроме того, на основе анализа логов сети в рамках тестового сценария проверяется наличие и полнота исходных данных — информационных признаков, необходимых для обнаружения атак, таких как wormhole и sinkhole, при помощи методов машинного обучения с учителем [3].

К основным выводам о применимости самоорганизующихся децентрализованных БСС можно отнести перспективность их использования в целях мониторинга физических объектов и территорий, характеризующихся высоким динамизмом наблюдаемых объектов и процессов.

Подверженность таких инфраструктур злонамеренным воздействиям со стороны атакующих с различными уровнем возможностей и типом доступа подтверждает их критичность по отношению к атакам, эксплуатирующим свойства самоорганизации и децентрализации, в том числе в целях повышения скрытности таких атак.

*Исследование выполнено за счет гранта Российского научного фонда № 24-21-00486, <https://rscf.ru/project/24-21-00486/>.*

## СПИСОК ЛИТЕРАТУРЫ

1. Saleh H. M., Marouane H., Fakhfakh A. Stochastic gradient descent intrusions detection for wireless sensor network attack detection system using machine learning // IEEe Access. 2024. T. 12. C. 3825-3836.
2. Desnitsky V., Kotenko I. Expert knowledge based design and verification of secure systems with embedded devices // Lecture Notes in Computer Science. 2014. T. 8708. C. 194-210.
3. Balueva A., Desnitsky V., Ushakov I. Approach to detection of denial-of-sleep attacks in wireless sensor networks on the base of machine learning // Studies in Computational Intelligence. 2020. T. 868. C. 350-355.

УДК 004.27

## О ВЛИЯНИИ АРХИТЕКТУРНЫХ РЕШЕНИЙ НА БЕЗОПАСНОСТЬ ПРИНЯТИЯ РЕШЕНИЙ В ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМАХ

Дубенецкий Владислав Алексеевич, Кузнецов Александр Григорьевич,  
Цехановский Владислав Владимирович

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)  
Профессора Попова ул., 5, Санкт-Петербург, 197022, Россия  
e-mails: dubvl@list.ru, agkuznetcov@etu.ru, vvcehanovsky@mail.ru

**Аннотация.** Рассматриваются архитектурные решения информационных систем, обеспечивающие повышение уровня безопасности принятия решений за счет динамического поддержания в актуальном состоянии системы правил и ограничений проверки корректности и допустимости решений.

**Ключевые слова:** архитектура системы; классификатор объектов; ролевые структуры; правила и ограничения принятия решений.

## ON THE INFLUENCE OF ARCHITECTURAL DECISIONS ON THE SECURITY OF DECISION-MAKING IN INFORMATION AND CONTROL SYSTEMS

Dubenetsky Vladislav, Kuznetsov Alexander, Tsechanovsky Vladislav

Saint Petersburg Electrotechnical University  
5 Professora Popova St., St. Petersburg, 197022, Russia  
e-mails: dubvl@list.ru, agkuznetcov@etu.ru, vvcehanovsky@mail.ru

**Abstract.** The article examines architectural solutions for information systems that ensure an increased level of decision-making security by dynamically maintaining the system of rules and restrictions for checking the correctness and admissibility of decisions in an up-to-date state.

**Keywords:** system architecture; object classifier; role structures; decision-making rules and constraints.

В настоящее время управление деятельностью в различных областях все в большей степени поддерживается цифровыми приложениями различной степени сложности. Ярким примером является использование в производстве систем управления ресурсами. В таких системах логика принятия решений частично реализована в программах и данных системы управления, многие решения могут приниматься автоматически или через их подтверждение пользователями. Логика принятия решения распределена в коде приложения и даже при тщательном тестировании не может гарантировать полноту и безопасность формируемых решений. Кроме того, развитие бизнеса требует внесение изменений путем не только параметрической, но и структурной настройки ограничений и правил принятия решений. Существует проблема обеспечения безопасности принятия решений в информационно-управляющих системах (ИУС). Цена ошибки в принятии решения может очень высокой. Как правило, модель предметной области в таких системах растворена в метаданных базы данных и коде приложения, имеющиеся точки расширения и настройки позволяют вносить изменения только на периоде компиляции. В этой связи актуальной является задача разработки такой технологии создания ИУС, которая обеспечит доступ к ограничениям и правилам принятия решений на периоде исполнения специалистам предметной области и позволит им поддерживать и контролировать логику принятия решений в процессе сопровождения приложения.

Общие вопросы архитектурного проектирования и реализации с использованием моделей, допускающих исполнение рассмотрены в [1]. В данном докладе освещается вопрос использования модели предметной области при разработке такой архитектуры приложения, которая обеспечит повышение безопасности принятия решений за счет предоставления сервисов управления правилами и ограничениями на периодах настройки, внедрения и сопровождения приложений.

Чтобы справиться с потоком изменений и расширений предлагается архитектурное решение, основанное на явном включении в состав приложения конструкторов и исполнителей объектной модели предметной области (ОМПО), которые обеспечат поддержание соответствия изменяющейся реальности в границах проекта и ОМПО. В [1] такой компонент назван *Фабрика инструментов*. Первыми кандидатами на поддержку являются классификаторы компонентов, роли и правила.

Классификаторы объектов, процессов, событий, изделий, документов, заказов, хозяйственных операций, субъектов деятельности и других компонентов домена предметной области в границах проекта обеспечивают высокий уровень структурирования проектных решений. Каждый такой классификатор является хорошей точкой расширения приложения. Статическая модель задает ряд ограничений для модели поведения. Для описания поведения предлагается включать в приложение конструктор и исполнитель логики поведения объектов [2].

Для описания логики используется модель коллективного поведения автоматов. Конструктор позволяет на этапе исполнения описать шаблон модели поведения каждого класса объектов используя правила как синхронного, так и асинхронного взаимодействия, а также учитывать в сторожевых условиях состояния взаимодействующих объектов и правила назначения объектов на роли [3]. Для вычисления значения сторожевого условия необходимо знать следующие фактические параметры текущего состояния экземпляра процесса: типовое состояние в текущей позиции; типовое решение, принимаемое в текущей позиции; результаты контроля

значений параметров объекта, к которому привязан процесс; идентификатор сотрудника, который принимает решение в текущем состоянии. Для экземпляра процесса известны шаблон и траектория с указанием текущего состояния. Обычно существует некоторая базовая настройка классификации компонентов. Все расширения рассматриваются как конкретизация базовых компонентов. Конструктор ролевых структур опирается на классификатор компонентов и некоторый предопределенные классы ролей.

Конструктор процессов позволяет формировать шаблоны процессов, описывать логику переходов и взаимную синхронизацию для классов объектов и ролей. Классификатор процессов первоначально содержит описание нескольких базовых шаблонов. Специалист предметной области при определенной подготовке способен самостоятельно работать с конструкторами моделей, встроенными в приложение, и имеющими доброжелательный интерфейс. Например, каждый специалист формирует свою часть конструкторско-технологической спецификации изделий в части их касающейся. Аналогично формируются ролевые структуры, классификаторы и шаблоны процессов.

Выделяются классы пассивных и активных объектов. Траектория жизненного цикла (ЖЦ) пассивных объектов формируется управляющими объектами, принимающими решения в каждом из текущем состоянии пассивного объекта. Обычно решения принимаются пользователями приложения, имеющими соответствующие права доступа. Движение объекта может быть синхронизировано с состояниями других объектов различных классов, имеющих роли у основного класса. Таким образом, сложная логика коллективного поведения реализуется через логику поведения каждого объекта с включением в сторожевые условия данных связанных объектов. Траектория ЖЦ активных объектов формируется автоматически путем вычисления функций переходов, задающих правила перехода в следующее состояние, и отражающих принятое решение. В ряде случаев для перехода требуется подтверждение пользователей приложения.

Выбор состояний. Данные объектов разбиваются на группы в соответствии с областями знаний их поддерживающих. Состояния формируются на основе знаний узкой специализации экспертов. С каждым из состояний связывается набор функций, достаточных для формирования необходимых данных и проверки их корректности, и группа пользователей с соответствующими правами доступа. Некоторые состояния могут быть активизированы параллельно, другие связаны последовательной управляющей структурой. В процессе работы с объектом некоторые его свойства описываются через ассоциации с другими объектами. При назначении этих объектов на соответствующие роли в соответствующем шаблоне должны быть описаны ограничения на состояния и значения параметров. Таким образом, каждый объект в процессе своего жизненного цикла движется по некоторой траектории за счет принятых решений компетентными специалистами в части их касающихся. Совокупность правил разбивается на группы по классу объекта, его роли и состоянию.

Таким образом, для повышения безопасности принятия решений в ИУС предлагается в приложение включать:

- явно описанную модель предметной области с открытым для расширения *Классификатором объектов*, обеспечивающую строгую типизацию всех объектов и их свойств;
- конструкторы шаблонов для описания свойств и поведения объектов с разделением ответственности за принятые решения;
- конструкторы модели поведения с выделением состояний в соответствии с компетентностью пользователей по фрагментам предметной области;
- правила для описания логики поведения и проверки корректности принятия решений.

Предлагаемое архитектурное решение было использовано при разработке информационной системы класса ERP «РЕСУРС» (свидетельство об официальной регистрации программ для ЭВМ № 2007611351) и прошло многократную практическую проверку.

#### СПИСОК ЛИТЕРАТУРЫ

1. Водяхо А.И., Выговский Л.С., Дубенецкий В.А., Цехановский В.В. Архитектурные решения информационных систем: учебник для СПО / Санкт-Петербург: Лань, 2023. 356 с.
2. В.А. Дубенецкий Методика конструирования моделей этапов анализа и проектирования на основе образцов документов: учеб.-метод. пособие. СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2023. 40 с.
3. Дубенецкий В.А., Кузнецов А.Г., Цехановский В.В. Технология создания корпоративных информационно-управляющих систем на основе моделей, допускающих исполнение. СПб. Изд-во СПбГЭТУ «ЛЭТИ», 2019. 158 с.

УДК 003.26

#### **ВЫБОР СТЕПЕНИ РАСШИРЕНИЯ ДВОИЧНОГО ПОЛЯ ДЛЯ ЗАДАНИЯ ВЕКТОРНЫХ КОНЕЧНЫХ ПОЛЕЙ КАК НОСИТЕЛЕЙ ДВУХКЛЮЧЕВЫХ КРИПТОАЛГОРИТМОВ НА ТРУДНО ОБРАТИМЫХ ОТОБРАЖЕНИЯХ**

**Захаров Дмитрий Викторович, Молдовян Александр Андреевич, Молдовян Дмитрий Николаевич**  
СПб ФИЦ РАН

14-я линия В. О., 39, Санкт-Петербург, 199178, Россия  
e-mails: zakharov.dmitriy@gmail.com, maa1305@yandex.ru, mdn.spectr@mail.ru

**Аннотация.** Рассматривается вопрос выбора степени расширения  $s$  двоичного поля для задания над ним векторных конечных полей характеристики два, представляющих интерес для разработки на их основе

двухключевых криптоалгоритмов, основанных на трудно обратимых отображениях с секретной лазейкой. Обязательным требованием является обеспечение делимости порядка мультипликативной группы поля, являющегося расширением двоичного поля, на значение размерности  $m$  векторного конечного поля. Это требование определяет ограниченный набор возможных значений  $m$  для каждого фиксированного значения  $s$ . Для некоторых значений  $s$  все делители упомянутой группы являются настолько большими, что возможные значения  $m$  становятся непрактичными для разработки криптоалгоритмов из-за чрезмерно большого размера (увеличивающегося по квадратичному закону в зависимости от  $m$ ) открытого ключа. Одним из формальных ограничений на выбор значения  $s$  является взаимная простота порядка мультипликативной группы векторного конечного поля и степени, в которую возводится  $m$ -мерный при выполнении над ним нелинейного отображения. Последнее требование не позволяет использовать операцию возведения в куб в качестве нелинейного отображения при одновременном использовании четного значения параметра  $s$ .

**Ключевые слова:** компьютерная безопасность; криптография; постквантовая криптография; цифровая подпись; открытое шифрование; нелинейное отображение; конечная алгебра; векторные конечные поля.

## CHOICE OF THE EXTENSION DEGREE OF A BINARY FIELD FOR DEFINING VECTOR FINITE FIELDS AS SUPPORTS OF PUBLIC-KEY CRYPTALGORITHMS ON HARD-TO-INVERTIBLE MAPPINGS

Zakharov Dmitriy, Moldovyan Alexandr, Moldovyan Dmitriy

St. Petersburg Federal Research Center of the Russian Academy of Sciences

39, 14-th Linia, VI, St. Petersburg, 199178, Russia

e-mails: zakharov.dmitriy@gmail.com, maa1305@yandex.ru, mdn.spectr@mail.ru

**Abstract.** The problem of choosing the extension degree of a binary field for defining vector finite fields of characteristic two over it is considered. These fields are of interest for developing public-key cryptographic algorithms based on hard-to-reverse mappings with a secret trapdoor. A mandatory requirement is to ensure divisibility of the order of the multiplicative group of the field, which is an extension of the binary field, by the value of the dimension  $m$  of the vector finite field. This requirement defines a limited set of possible values of  $m$  for each fixed value of  $s$ . For some values of  $s$ , all divisors of the mentioned group are so large that the possible values of  $m$  become impractical for developing cryptographic algorithms due to the excessively large size of the public key, which grows according to the quadratic law depending on  $m$ . One of the formal restrictions on the choice of the value of  $s$  is the mutual primality of the order of the multiplicative group of the vector finite field and the power to which the  $m$ -dimensional vectors are exponentiated when performing a nonlinear mapping over it. The latter requirement does not allow using the operation of exponentiating to cube as a nonlinear mapping when simultaneously using an even value of the parameter  $s$ .

**Keywords:** computer security; cryptography; post-quantum cryptography; digital signature; public encryption; non-linear mapping; finite algebra; vector finite fields.

Двухключевые криптографические алгоритмы на трудно обратимых отображениях с секретной лазейкой представляют значительный интерес как постквантовые криптосхемы благодаря тому, что их стойкость основана на вычислительной трудности решения больших систем степенных уравнений (БССУ), для решения которой квантовый компьютер не является эффективным. Алгоритмы данного типа используют открытый ключ, заданный в виде набора многочленов над некоторым конечным полем (базовым полем) сравнительно малого порядка, а отображения выполняются над  $m$ -мерными векторами, координаты которых являются элементами базового поля. Выходным значением отображения является вектор, координаты которого вычисляются как значения многочленов, вычисленных от переменных, значения которых принимаются равными координатам входного вектора. Если многочлены открытого ключа представляют собой степенные многочлены (обычно второй степени), то отображение является нелинейным и его легко задать таким, что выполнение обратного отображения практически невыполнимо, если не знать некоторый секрет (секретную лазейку) [1, 2]. Изначально разработка нелинейных отображений предполагалась как задание нелинейного отображения  $N$ , для которого сравнительно легко устанавливается обратное отображение. На такое исходное отображение далее накладывается одно или два линейных отображения  $\Phi$  и  $\Psi$ , задаваемое набором линейных многочленов. Для данной суперпозиции составных отображений вычисляется набор степенных многочленов, задающих результирующее трудно обратимое отображение. Благодаря маскирующему линейному отображению, для результирующего отображения выполнение обратного отображения представляется вычислительно невыполнимым, если не знать секретной лазейки — маскирующего линейного отображения. Однако, использование одного или более маскирующих отображений приводит к сильному росту размера открытого ключа, который достигает нескольких мегабайт в известных криптоалгоритмах рассматриваемого типа. Действительно, для вычисления набора многочленов, реализующих, например, суперпозицию  $N\Psi$  координаты выходного вектора отображения  $N$  берутся в качестве переменных для набора многочленов отображения  $\Psi$ , что приводит к тому, что число слагаемых в результирующих многочленах становится примерно равным произведению числа слагаемых в многочленах отображения  $N$  на число слагаемых отображения  $\Psi$ . При этом число многочленов открытого ключа задает стойкость криптоалгоритма берется равным от 26 для задания

80-битного уровня стойкости, до 93 для 256-битного уровня стойкости при использовании базового конечного поля GF(256) [3].

Попыткой решить проблему чрезмерного размера открытого ключа явился новый подход [3] к разработке криптоалгоритмов на отображениях с секретной лазейкой, состоящий в использовании нелинейных отображений, заданных набором многочленов, реализующих операцию возведения в некоторую небольшую степень  $k$  в векторных конечных полях (ВКП) [4]. Возникающая проблема задания достаточно большого числа модификаций ВКП при фиксированной его размерности решается использованием унифицированных параметризуемых методов их задания [5, 6]. В подходе [3] используются отображения, обращение которых реализуется путем извлечения корней соответствующих степеней в конечном поле, т.е. путем выполнения вычислительно эффективной операции при известной модификации ВКП. Последняя является секретной и ее вычисление по набору многочленов, составляющих открытый ключ, является вычислительно сложным и связано с решением некоторой БССУ, связывающей коэффициенты многочленов со структурными константами, задающими секретную модификацию ВКП. Для повышения производительности разрабатываемых криптоалгоритмов представляет интерес задание ВКП над расширенными двоичными полями, что приводит к задаче формулировки требований к выбору значения степени  $s$  расширения последних. Рассмотрение этого вопроса привело к следующим основным требованиям:

1. Делимости порядка  $\omega$  мультипликативной группы поля, являющегося расширением двоичного поля и используемого в качестве базового поля для задания ВКП, на значение размерности  $m$  ВКП является принципиальным условием.

2. Наличие в разложении  $\omega$  делителей, имеющих сравнительно малый размер, который может быть выбран в качестве значения размерности ВКП.

3. Выполнимость равенства  $\text{НОД}(\omega, k) = 1$ , где НОД обозначает наибольший общий делитель. Взаимная простота порядка мультипликативной группы векторного конечного поля и степени, в которую возводится  $m$ -мерный при выполнении над ним нелинейного отображения.

Последнее требование всегда может быть формально выполнено путем выбора соответствующих значений  $k$ , однако на практике при больших значениях  $k$  размер открытого ключа сильно возрастает при использовании суперпозиции двух операций экспоненцирования в ВКП.

Третье требование не позволяет использовать значение  $k = 3$  при одновременном использовании четного значения параметра  $s$ , включая интересные для практических алгоритмических разработок значения

$$s = 16, 24, 32, 40 \text{ и } 64,$$

обуславливая необходимость выбора соответствующих альтернативных значений

$$s = 15, 21 \text{ (23)}, 32 \text{ (27)} \text{ и } 57 \text{ (63)}.$$

Для случая  $s = 8$  приемлемая альтернатива отсутствует.

*Работа поддержана грантом РНФ № 24-41-04006, <https://rscf.ru/project/24-41-04006/>.*

#### СПИСОК ЛИТЕРАТУРЫ

1. Ding J., Petzoldt A., Schmidt D.S. Multivariate Cryptography // Multivariate Public Key Cryptosystems. Advances in Information Security. Springer, New York. 2020. V. 80. P. 7-23.
2. Hashimoto, Y. Recent Developments in Multivariate Public Key Cryptosystems / Takagi T., Wakayama M., Tanaka K., Kunihiro N., Kimoto K., Ikematsu Y. (eds) // International Symposium on Mathematics, Quantum Theory, and Cryptography. Mathematics for Industry. Springer, Singapore. 2021. V. 33. P. 209-229.
3. Ding J., Petzoldt A. Current State of Multivariate Cryptography // IEEE Security and Privacy Magazine. 2017. Vol. 15. № 4. Pp. 28-36.
4. Молдовян А. А., Молдовян Д. Н., Молдовян Н. А. Новый подход к разработке алгоритмов многомерной криптографии // Вопросы кибербезопасности. 2023. № 2(54). С. 52-64. DOI:10.21681/2311-3456-2023-2-52-6.
5. Moldovyan N. A. Parameterized method for specifying vector finite fields of arbitrary dimensions // Quasigroups and related systems. 2024. Vol. 32. № 2. Pp.299-312. <https://doi.org/10.56415/qrs.v32.21>.
6. Moldovyan A. A., Moldovyan N. A. Parameterized unified method for setting vector finite fields for multivariate cryptography // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2024. Т. 20. Вып. 4. С. 479-486. <https://doi.org/10.21638/spbu10.2024.404>.

УДК 004.852

#### АНАЛИЗ АЛГОРИТМОВ ФЕДЕРАТИВНОЙ КЛАСТЕРИЗАЦИИ

**Забалуев Даниил Антонович, Колпашиков Максим Алексеевич**

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

Профессора Попова ул., 5, Санкт-Петербург, 197022, Россия

e-mails: [dazabaluev@stud.etu.ru](mailto:dazabaluev@stud.etu.ru), [makolpashikov@gmail.com](mailto:makolpashikov@gmail.com)

**Аннотация.** Методы федеративной кластеризации обучения позволяют выполнить кластеризацию данных, распределенных по разнородным вычислительным устройствам, таким как мобильные телефоны, носимые интеллектуальные устройства, центры обработки данных. В докладе авторы исследуют различные подходы и алгоритмы федеративной кластеризации, изучают их преимущества и формулируют открытые проблемы их применения на практике. Особое внимание уделяется применению алгоритмов в условиях неидентично распределенных данных и неоднородных вычислительных ресурсов.

**Ключевые слова:** федеративное обучение; кластеризация; обработка неидентично распределенных данные; машинное обучение.

## ANALYSIS OF THE FEDERATED CLUSTERING ALGORITHMS

**Zabaluev Daniil, Kolpashikov Maxim**

St. Petersburg State Electrotechnical University «LETI»

5 Professor Popov St, St. Petersburg, 197022, Russia

e-mails: dazabaluev@stud.etu.ru, makolpashikov@gmail.com

**Abstract.** The methods of federated learning clusterization allow clustering of data distributed across heterogeneous computing devices such as mobile phones, wearable smart devices, and data centers. In the report, the authors explore various approaches and algorithms of federated clustering, explore their advantages and formulate open problems of their application in practice. Particular attention is paid to the use of algorithms in conditions of non-identically distributed data and heterogeneous computing resources.

**Keywords:** federated learning; clusterization; non-IID data processing; machine learning.

Задача применения технологий искусственного интеллекта на практике связана с наличием доступа к большим обучающим выборкам [1]. Качество обучающей выборки определяет точность решения аналитической задачи методами глубокого обучения. Часто возникает задача анализа данных пользователей различных информационных систем или организаций при построении рекомендательных систем, проведении маркетинговых кампаний и т.д. Однако их использование сопряжено с рядом проблем. Рост утечек и случаев неправомерного использования персональных данных и других видов конфиденциальной информации привел к ужесточению законодательной базы, направленной на обеспечение защиты информации такого рода. Так, за последние пять лет было принято и дополнено несколько федеральных законов, направленных на защиту персональных данных граждан РФ. Например, федеральный закон от 8 августа 2024 г. №233-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» и Федеральный закон «О проведении эксперимента ... и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» [2] накладывает серьезные ограничения на хранение и передачу персональных данных:

- чувствительные данные нельзя просто собрать в одном месте и обучить модель — необходимо произвести предварительное обезличивание данных, либо получить от владельца данных согласие на их использование, что является сложной и времязатратной задачей;

- чувствительные данные граждан РФ должны храниться исключительно на территории РФ.

Таким образом, компании и организации, оперирующие персональными данными и/или предоставляющих персонализированные информационные сервисы, вынуждены искать новые технологические решения для работы с конфиденциальной информацией с использованием методов искусственного интеллекта и машинного обучения. Одной из наиболее распространенной технологий, обеспечивающих конфиденциальность данных при их распределенном анализе, является технология федеративного машинного обучения — при федеративном обучении чувствительные данные остаются «на месте», поскольку обучение производится локально, а в центры обработки данных попадают только градиенты или обновления весов модели.

В настоящее время в научной литературе представлены различные алгоритмы федеративного обучения для решения задач классификации, регрессии, кластеризации. Классическим алгоритмом федеративного обучения, который используется для формирования модели анализа, является алгоритм федеративного обучения *FedAvg*. Он по своей сути является достаточно простым и вычислительно эффективным, однако точность его работы сильно падает в условиях неидентично распределенных (non independent and identically distributed, non-IID) данных. Значимая часть исследований посвящена разработке эффективных методов агрегации для не идентично распределенных данных. Примером таких алгоритмов являются алгоритмы *FedProx*, *FedBN*, которые более устойчивы в условиях гетерогенных данных и устройств, однако более сложны в настройке [3]. Следует также отметить, что предложения решения в основном предназначены для классификации объектов, в т. ч. изображений.

Для решения задачи федеративной кластеризации также предложены разнообразные алгоритмы, например, *GMM* [4], *CADIS* [5], *FL+HC* [6]. В основе *GMM* (Generalized Method of Moments) лежит классический алгоритм кластеризации *k-means*, однако инициализация средних значений, расчет ковариации и веса осуществляется на сервере. При обучении указанные параметры передаются клиентам, где они пересчитываются и возвращаются на централизованный узел для последующей агрегации и усреднения [4]. Агрегация значений осуществляется путем вычисления средневзвешенных значений, обновленных средних от всех клиентов. В алгоритмах *F-FCM* [7] и *FFCM* [8] применены методы нечеткой кластеризации для повышения защиты конфиденциальности, в них передается только информация о принадлежности объекта к кластеру. В [9] предложено использовать методы подпространственной кластеризации (subspace clustering), которые разработаны для кластеризации многомерных данных, поскольку во многих приложениях многомерные данные могут быть хорошо представлены объединением низкоразмерных подпространств. *FedGMCC* (Federated Geometric Monte Carlo Clustering) [10] — метод, применяющий геометрический подход для оценки схожести моделей клиентов, используя методы Монте-Карло для анализа выходного пространства моделей и их геометрических связей. Данный подход позволяет эффективно обучать модели в условиях non-IID данных [6].

Геометрические связи между моделями определяются с помощью аффинных кривых, что позволяет выявить «связанные» модели; и выполнять их агрегация с учетом связности.

Многообразие существующих методов федеративного обучения обуславливает необходимость анализа и систематизации полученных результатов для определения оптимальных условий их применения в практических задачах и выбора их настроек. С этой целью авторы сформировали следующие вопросы, представляющие интерес для исследования:

- Какие типы алгоритмов кластеризации адаптированы для федеративного обучения?
- Какие механизмы разработаны для оптимизации алгоритмов агрегирования результатов в условиях неидентично распределенных данных?
- Каким образом определяется число кластеров в данных, распределенных между клиентами?
- Каким образом учитывается неоднородность коммуникационных возможностей клиентов?
- Для данных какой модальности разработаны алгоритмы?
- Какие сценарии тестирования предложены для оценки эффективности кластеризации?
- Какие метрики используются для их оценки?
- Каким образом оценивается коммуникационная сложность алгоритмов, какие механизмы оптимизации предложены для снижения числа раундов агрегации?

Данные вопросы определили критерии оценки разработанных подходов к федеративной кластеризации. Поиск работ осуществлялся по англоязычным библиографическим системам и русскоязычной научной библиотеке eLibrary, по ключевым словам, «федеративное обучение», «кластеризация», «федеративная кластеризация». Из рассмотрения были исключены работы, в которых алгоритмы кластеризации применяются как механизм обработки неоднородности в данных.

В докладе обсуждаются результаты выполненного исследования, формулируются их основные свойства и формулируются основные открытые задачи, которые определяют дальнейшие направления исследования в области алгоритмов федеративной кластеризации.

*Работа выполнена при поддержке гранта Российского научного фонда № 25-11-20020 (<https://rscf.ru/project/25-11-20020/>) и Санкт-Петербургского научного фонда.*

#### СПИСОК ЛИТЕРАТУРЫ

1. Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» URL: <https://www.it-grad.ru/blog/obrabotka-i-zashhita-personalnykh-dannykh-chasto-zadavaemye-voprosy> (дата обращения: 08.08.2025).
2. Федеральный закон от 8 августа 2024 г. № 233-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» и Федеральный закон «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации - городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» // Официальный интернет-портал правовой информации. 2024. URL: <https://publication.pravo.gov.ru/Document/View/0001202408080031> (дата обращения: 09.08.2025).
3. Z. Lu, H. Pan, Y. Dai, X. Si and Y. Zhang, «Federated Learning With Non-IID Data: A Survey», in *IEEE Internet of Things Journal*, vol. 11, no. 11, pp. 19188-19209, 1 June 1, 2024, doi: 10.1109/IJOT.2024.3376548.
4. Li C. et al. High-Precision Cluster Federated Learning for Smart Home: An Edge-Cloud Collaboration Approach // *IEEE Access*. 2023. Vol. 11. P. 102157-102168. doi: 10.1109/ACCESS.2023.3315771.
5. Nguyen T. et al. Cadis: Handling cluster-skewed non-iid data in federated learning with clustered aggregation and knowledge distilled regularization // 2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing (CCGrid). IEEE, 2023 P. 249-261.
6. Briggs C., Fan X., Andras P. Federated Learning with Hierarchical Clustering of Local Updates to Improve Training on Non-IID Data // 2020 international joint conference on neural networks (IJCNN). IEEE, 2020. P. 1-9. doi: 10.1109/IJCNN48605.2020.9207469.
7. Pedrycz, W. 2022. Federated FCM: Clustering under privacy requirements. *IEEE Transactions on Fuzzy Systems*, 30(8): 3384–3388.
8. Stallmann, M.; and Wilbik, A. 2022. Towards federated clustering: A federated fuzzy c-means algorithm (FFCM). *arXiv:2201.07316*.
9. Xie, S.; Wu, Y.; and Liao, e. a., Kewen. 2023. Fed-SC: Oneshot federated subspace clustering over high-dimensional data. In 2023 International Conference on Data Engineering, 2905–2918.
10. Lucchetti D., Roy A., Mahmoud H. Federated geometric monte carlo clustering to counter non-iid datasets // *arXiv preprint arXiv:2204.11017*. 2022. doi: 10.48550/arXiv.2204.11017.

УДК 003.26

#### КОНЕЧНЫЕ АЛГЕБРЫ МАТРИЦ КАК НОСИТЕЛИ АЛГОРИТМОВ ЭЦП СО СКРЫТОЙ ГРУППОЙ

Захаров Дмитрий Викторович<sup>1</sup>, Молдовян Дмитрий Николаевич<sup>2</sup>, Молдовян Николай Андреевич<sup>1</sup>

<sup>1</sup> СПб ФИЦ РАН

14-я линия В. О., 39, Санкт-Петербург, 199178, Россия

<sup>2</sup> Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

Профессора Попова ул., 5, Санкт-Петербург, 197022, Россия

e-mails: zakharov.dmitriy@gmail.com, mdn.spectr@mail.ru, nmold@mail.ru

**Аннотация.** Алгебраические алгоритмы ЭЦП со скрытой группой, основанные на вычислительной трудности решения больших систем степенных уравнений в конечном поле, представляют значительный практический интерес как постквантовые криптосхемы. В них в качестве алгебраического носителя используются многомерные конечные некоммутативные ассоциативные алгебры, заданные над базовым конечным полем. Уровень стойкости таких алгоритмов в значительной степени определяется размерностью алгебр. Для больших значений размерности могут быть использованы некоторые известные унифицированные способы задания алгебр указанного типа. Однако эти способы приводят к построению  $m$ -мерных алгебр, в которых операция умножения векторов осуществляется путем выполнения  $m \times m$  операций умножения в базовом



поле. Для повышения производительности алгебраических алгоритмов ЭЦП предлагаются альтернативные их носители -- конечные алгебры матриц  $n \times n$ , которые могут быть рассмотрены как векторы размерности  $m = n \times n$ . При этом матричное умножение выполняется за  $n \times n \times n$  умножений в базовом поле и порядок базового поля может быть легко выбран таким, что в алгебре матриц будут существовать и легко могут быть сгенерированы невырожденные матрицы простых порядков достаточно большого размера. Показано, что для применения в качестве носителя упомянутых алгоритмов представляю интерес конечные алгебры матриц размеров, соответствующих значениям  $n = 3, 4, 5, 6$  и  $7$ .

**Ключевые слова:** компьютерная безопасность; криптография; постквантовая криптография; цифровая подпись; алгоритмы ЭЦП; конечные алгебры матриц.

## FINITE MATRIX ALGEBRAS AS ALGEBRAIC SUPPORTS OF DIGITAL SIGNATURE ALGORITHMS WITH A HIDDEN GROUP

Zakharov Dmitriy<sup>1</sup>, Moldovyan Dmitriy<sup>2</sup>, Moldovyan Nikolay<sup>1</sup>

<sup>1</sup> St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS),  
39 14-th Linia, VI, St. Petersburg, 199178, Russia

<sup>2</sup> Saint Petersburg Electrotechnical University

5 Professor Popov St, St. Petersburg, 197022, Russia

e-mails: zakharov.dmitriy@gmail.com, mdn.spectr@mail.ru, nmold@mail.ru

**Abstract.** Algebraic digital signature algorithms with a hidden group, which are based on the computational difficulty of solving large systems of power equations in a finite field, are of considerable practical interest as post-quantum cryptoschemes. Multidimensional finite non-commutative associative algebras defined over a base finite field are used as algebraic supports in algorithms of such type. The security level of such algorithms is largely determined by the dimension of the said algebras. For large values of the dimension  $m$ , some known unified methods for defining algebras of the indicated type can be used. However, that methods lead to the construction of  $m$ -dimensional algebras, in which the vector multiplication operation is performed by performing  $m \times m$  multiplication operations in the base field. To improve the performance of algebraic digital signature algorithms, alternative supports are proposed -- finite algebras of the  $n \times n$  matrices, which can be considered as vectors of dimension  $m = n \times n$ . In this case, matrix multiplication is performed in  $n \times n \times n$  multiplications in the base field. Besides, the order of the base field can be easily chosen such that non-singular matrices of prime orders of sufficiently large size will exist and can be easily generated in the matrix algebras. It is shown that finite algebras of matrices of sizes corresponding to the values  $n = 3, 4, 5, 6$ , and  $7$  are of interest for use as carriers of the above algorithms.

**Keywords:** computer security; cryptography; post-quantum cryptography; digital signature; public encryption; vector finite fields.

Алгебраические алгоритмы ЭЦП со скрытой коммутативной группой [1, 2] являются новым типом постквантовых криптосхем, стойкость которых основана на вычислительной сложности решения больших систем степенных уравнений (БССУ). В сравнении с известными постквантовыми алгоритмами ЭЦП, включая недавно предложенные проекты постквантовых стандартов ЭЦП, они обладают существенно меньшими размерами открытого ключа и подписи, благодаря чему представляют значительный интерес для ряда потенциальных практических применений. В упомянутых алгоритмах ЭЦП в качестве алгебраического носителя используются конечные некоммутативные ассоциативные алгебры (КНАА) с глобальной двухсторонней единицей [3, 4]. Обычно КНАА задаются путем определения дополнительной операции в конечном векторном пространстве, а именно операции векторного умножения, которая выполняется как перемножение каждой компоненты первого вектора-множителя с каждой компонентой второго. При этом результат каждого из таких вспомогательных умножений задается как однокомпонентный вектор в соответствии с так называемой таблицей умножения базисных векторов (ТУБВ). Если построить ТУБВ, которая задаст операцию векторного умножения, обладающую свойствами замкнутости, двухсторонней дистрибутивности относительно операции сложения векторов, ассоциативности и некоммутативности, то будем иметь некоторую  $m$ -мерную КНАА. Существуют КНАА с большим числом глобальных односторонних (правосторонних или левосторонних) единиц и с единственной глобальной двухсторонней единицей. Последние представляют наибольший интерес в качестве носителя алгебраических алгоритмов ЭЦП со скрытой коммутативной группой, стойкость которых основана на вычислительной трудности решения БССУ. Уровень стойкости таких алгоритмов во многом определяется размерностью КНАА, поскольку число уравнений в БССУ находится в пропорциональной или близкой к пропорциональной зависимости от значения  $m$ . Построение многомерных КНАА с глобальной двухсторонней единицей является неочевидным, но существуют унифицированные способы задания КНАА с глобальной двухсторонней единицей [5, 6], которые могут быть использованы для разработки алгоритмов ЭЦП, обладающих 256-битным уровнем стойкости.

Однако, эти унифицированные способы приводят к заданию операции векторного умножения, вычислительная сложность которой примерно равна  $m \times m$  умножениям в базовом конечном поле, т.е. в поле, над которым задана КНАА.

Для повышения производительности процедур генерации и верификации ЭЦП в рассматриваемых алгоритмах представляет интерес использование конечных алгебр матриц размера  $n \times n$  с операцией матричного

умножения, имеющей сложность, примерно равную  $n \times n \times n$  умножениям в базовом конечном поле. При этом замена алгебраического носителя в известных алгоритмах ЭЦП со скрытой коммутативной группой [7–9] на конечную алгебру матриц приводит в рамках прямой атаки к решению БССУ с числом уравнений равным  $n \times n$ . Действительно, алгебру матриц размера  $n \times n$  можно трактовать как КНАА размерности  $m = n \times n$ , заданную по специальной прореженной ТУБВ, которая легко записывается с учетом правила матричного умножения. При этом известна формула, описывающая значение порядка матриц по значению порядка базового поля, из которой следует существование матриц, обладающих порядком достаточно большого размера, и возможностью выбора порядка базового конечного поля таким, что порядок указанных матриц будет содержать простой делитель достаточно большой разрядности.

При разработке алгоритмов ЭЦП последнее обстоятельство позволяет использовать алгебры матриц, заданные над конечными полями порядков, имеющих разрядность 64 бит (при  $n = 3$ ), 32 бит (при  $n = 5$ ) и 16 бит (при  $n = 7$ ), потенциально обеспечивая 256-битную стойкость. Представляет интерес также и использование матриц размеров  $4 \times 4$  и  $6 \times 6$ , однако следует учитывать, что в них максимальный простой порядок матриц ограничен значениями простых порядков матриц для случаев  $n = 3$  и  $n = 5$ . Это легко показать, рассматривая диагонально клеточные матрицы соответствующих размеров. Используя такое представление и учитывая отображения автоморфизма, можно легко установить значения порядков существующих коммутативных подгрупп мультипликативной группы, заданной алгебры матриц.

С целью повышения производительности алгоритмов ЭЦП и снижения сложности их аппаратной реализации представляет интерес использование в качестве алгебраического носителя конечных алгебр матриц  $n \times n$ , заданных над конечными полями четной характеристики, с простыми значениями  $n$ .

*Работа поддержана грантом РНФ № 24-41-04006, <https://rscf.ru/project/24-41-04006/>.*

#### СПИСОК ЛИТЕРАТУРЫ

1. Молдовян Д. Н., Молдовян А. А. Алгебраические алгоритмы ЭЦП, основанные на трудности решения систем уравнений // Вопросы кибербезопасности. 2022. № 2 (48). С. 7–17. DOI: 10.21681/2311-3456-2022-2-7-17.
2. Молдовян А. А., Молдовян Н. А. Алгоритмы ЭЦП на конечных некоммутативных алгебрах над полями характеристики два // Вопросы кибербезопасности. 2022. № 3(49). С. 58–68. DOI: 10.21681/2311-3456-2022-3-58-68.
3. Duong M. T., Moldovyan D. N., Do B. V., Nguyen M. H. Post-quantum signature algorithms on noncommutative algebras, using difficulty of solving systems of quadratic equations // Computer Standards and Interfaces. 2023. V. 86. Pp. 103740. DOI: 10.1016/j.csi.2023.103740.
4. Moldovyan N. A. Algebraic signature algorithms with a hidden group, based on hardness of solving systems of quadratic equations // Quasigroups and Related Systems, 2022. Vol. 30. № 2(48). Pp. 287–298. DOI: 10.56415/qrs.v30.24.
5. Moldovyan N. A. Unified Method for Defining Finite Associative Algebras of Arbitrary Even Dimensions // Quasigroups and related systems. 2018. V. 26. № 2. Pp. 263–270.
6. Dinh K.-L., Nguyen L.-G., Do T.-B., Moldovyan A. A., Moldovyan D. N., Kostina A. A. Defining high-dimensional non-commutative algebras as carriers for post-quantum digital signature algorithms // Proc. of the 1st International Conference on cryptography and information security (VCRIS). Hanoi, Vietnam, 2024. Pp. 1–5. DOI: 10.1109/VCRIS63677.2024.10813386.
7. Молдовян Н. А., Петренко А. С. Алгебраический алгоритм ЭЦП с двумя скрытыми группами // Вопросы кибербезопасности. 2024. № 6 (64). С. 98–107. DOI: 10.21681/2311-3456-2024-6-98-107.
8. Moldovyan A. A., Moldovyan N. A. A method for enhancing randomization in algebraic signature algorithms on non-commutative algebras // Quasigroups and related systems. 2025. V. 33. № 1. Pp. 71–83. DOI: 10.56415/qrs.v33.06.
9. Duong M. T., Moldovyan A. A., Moldovyan D. N., Nguyen M. H., Do T.-B. Structure of quaternion-type algebras and a post-quantum signature algorithm // International Journal of Electrical and Computer Engineering (IJECE). 2024. V. 15. № 3. Pp. 2965–2976. DOI: 10.11591/ijece.v15i3.pp2965-2976.

УДК 004.056

#### СОСТЯЗАТЕЛЬНЫЕ АТАКИ НА ВХОДНЫЕ ДАННЫЕ НЕЙРОННОЙ СЕТИ РАСПОЗНАВАНИЯ: ТЕОРИЯ И ЭКСПЕРИМЕНТ

**Зеленцова Елена Викторовна, Виткова Лидия Андреевна**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

e-mails: elena.zel@mail.ru, vitkova.la@sut.ru

**Аннотация.** В работе рассмотрены ключевые понятия, связанные с состязательными атаками на входные данные нейронных сетей распознавания изображений. Также в рамках текущего доклада проведен практический эксперимент, который моделирует состязательный тип атаки на два разных типа входных данных: изображение, на котором нейронная сеть была обучена ранее и на новое для модели изображение. Эксперимент позволил сделать выводы об эффективности данного типа атак в разных условиях.

**Ключевые слова:** нейронные сети; инциденты безопасности; состязательные атаки; атаки данных; информационная безопасность.

#### ADVERSARIAL ATTACKS ON THE INPUT DATA OF THE ARTIFICIAL NEURAL RECOGNITION NETWORK: THEORY AND EXPERIMENT

**Zelentsova Elena, Vitkova Lidia**

The Bonch-Bruевич Saint Petersburg State University of Telecommunications

22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia

e-mails: elena.zel@mail.ru, vitkova.la@sut.ru

**Abstract.** The paper discusses key concepts related to adversarial attacks on the input data of neural image recognition networks. Also, there was the practical experiment which simulates an adversarial type of attack on two different types of input data: an image on which the neural network was trained earlier and an image which is new for the model. The experiment allows to draw the conclusions about the effectiveness of this type of attack in different conditions.

**Keywords:** neural networks; security incidents; adversarial attacks; data attacks; information security.

В условиях стремительного развития технологий искусственного интеллекта растёт потребность в обеспечении его устойчивости к различным типам уязвимостей: как атак на входные или выходные данные, так и атак на саму модель. В рамках текущего доклада будут рассматриваться нейронные сети распознавания графических изображений и, в частности, атаки на данные, подающиеся на вход нейронной сети — рисунки, которые подлежат дальнейшей обработке искусственным интеллектом.

Особую угрозу в этом случае представляют состязательные атаки, или adversarial attacks [1], при которых минимальные и незаметные для человеческого восприятия изменения первоначальных данных, использующихся в качестве входных для нейронных сетей, приводят к ошибочной работе всей модели. Это может создать опасные предпосылки для возникновения инцидентов безопасности в любых сферах, где используется искусственный интеллект визуального распознавания. Подобный пример уже был продемонстрирован в реальных условиях: незначительные изменения изображений дорожных знаков привели к неверному их распознаванию автономными автомобилями [2].

Цель доклада — показать уязвимость моделей нейронных сетей распознавания изображений к Adversarial Attack через практический эксперимент.

Состязательные атаки реализуются с учетом различного уровня доступа к атакуемой модели. В случае, если атакующий обладает полной информацией о структуре нейронной сети, будет реализована атака белого ящика. Если доступ ограничен только взаимодействием с входными и выходными данными, выбирается атака черного ящика. Однако, на практике наиболее распространены атаки серого ящика, при которых атакующий владеет частичной информацией о параметрах нейронной модели или характере используемого набора данных.

В рамках исследования была воспроизведена состязательная атака на модель ResNet-50, обученную на датасете Imagenet. В качестве метода формирования искажённых данных был применён Fast Gradient Sign Method, или FGSM.

Классическая FGSM-атака [3] формулируется как задача максимизации функции потерь модели по отношению к входу при ограничении «бюджета» искажения. Простыми словами — атака добавляет к каждому пикселю изображения небольшой направленный «шум», вектор которого указывает, в какую сторону изменить пиксель, чтобы вероятность ошибки нейросети стала выше. Параметр  $\epsilon$  (эпсилон) в математическом представлении задачи задает силу искажений. Чем меньше данный параметр, тем незаметнее изменения для человеческого восприятия, но и эффект атаки в случае наименьших значений эпсилон также становится слабее.

В первом этапе эксперимента использовалось изображение кошки, ранее присутствующее в датасете, на котором ResNet-50 была обучена. Исходная классификация модели определила объект, как «полосатый кот». После внесения адверсариальных искажений с параметром  $\epsilon = 0.9$  результат изменился на «тойгер» (порода кошки, полосатый кот). Предсказание сместилось в близкую к верной категорию, поэтому такую атаку нельзя назвать полностью успешной, несмотря на изменения выходного результата. Было принято решение расширить эксперимент вторым этапом.

Во втором этапе эксперимента использовалось уникальное новое фото кота, ранее не встречавшееся в обучающем наборе. Изначально модель отнесла изображение к классу «коала». После применения атаки с параметром  $\epsilon = 0.9$ , аналогично предыдущей попытке, результат сместился к абсолютно противоположной категории — «кожистая черепаха».

Таким образом, результаты моделирования состязательной атаки продемонстрировали, что несмотря на незначительность вносимых изменений, воздействие на входные данные атакующим может существенно изменить конечное поведение модели распознавания, приводя к неверным предсказаниям на выходе. При этом устойчивость к атакам будет выше, если подающиеся на вход данные схожи с теми, которые модель уже встречала ранее в своем обучающем наборе.

Полученные результаты указывают на необходимость разработки комплексных мер защиты от состязательных атак, направленных на устойчивость нейронных моделей. К числу таких мер относятся внедрение методов регуляризации, использование устойчивых архитектур систем, мониторинг входных данных на программном уровне и обнаружение аномалий.

#### СПИСОК ЛИТЕРАТУРЫ

1. Goodfellow, I., Shlens, J., Szegedy, C. Explaining and Harnessing Adversarial Examples [Электронный ресурс] // URL: <https://arxiv.org/abs/1412.6572> (дата обращения: 21.08.2025).
2. Eykholt, K., Evtimov, I., Fernandes, E., Li, B., Rahmati, A., Xiao, C., Prakash, A., Kohno, T., Song, D. Robust Physical-World Attacks on Deep Learning Models [Электронный ресурс] // URL: <https://arxiv.org/abs/1707> (дата обращения: 21.08.2025).
3. Разработка защищенного веб-приложения: полное практическое руководство // Habr. 2018. URL: <https://habr.com/ru/companies/dsec/articles/437092/> (дата обращения: 15.08.202).

УДК 004.056

## ВЫЯВЛЕНИЕ МНОГОШАГОВЫХ КИБЕРАТАК В КОМПЬЮТЕРНЫХ СЕТЯХ НА ОСНОВЕ КОМБИНИРОВАНИЯ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ И ОБРАБОТКИ БОЛЬШИХ ДАННЫХ

Зеличенко Игорь Юрьевич, Котенко Игорь Витальевич

СПб ФИЦ РАН к

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия

e-mails: zelichenok@comsec.spb.ru, ivkote@comsec.spb.ru

**Аннотация.** Многошаговые кибератаки представляют серьезную угрозу информационной безопасности, особенно в условиях увеличивающегося объема и сложности сетевых данных. В работе предложен подход к обнаружению таких атак, основанный на комбинации методов интеллектуального анализа данных, включая модели машинного обучения, и технологий обработки больших данных. Разработана методика, включающая алгоритмы краткосрочного и долгосрочного анализа событий, реализованных с помощью двух LSTM-моделей. Построена модульная архитектура системы обнаружения, учитывающая высокую нагрузку и необходимость работы в режиме реального времени. Результаты экспериментальной апробации показали высокую точность (до 99%/82%  $f_1$  в задачах бинарной/многоклассовой классификации) и своевременность (30 сек. моментальный анализ/7 дней исторический) выявления атак как в стандартных компьютерных сетях, так и в IoT-средах.

**Ключевые слова:** информационная безопасность; многошаговые атаки; машинное обучение; Big Data; LSTM; потоковая обработка данных.

## DETECTING MULTI-STEP CYBER-ATTACKS IN COMPUTER NETWORKS BASED ON A COMBINATION OF MACHINE LEARNING AND BIG DATA PROCESSING METHODS

Zelichenok Igor, Kotenko Igor

St. Petersburg Federal Research Center of the Russian Academy of Sciences

39 14th Line VO, St. Petersburg, 199178, Russia

e-mails: zelichenok@comsec.spb.ru, ivkote@comsec.spb.ru

**Abstract.** Multi-stage cyberattacks pose a serious threat to information security, especially in the context of increasing volume and complexity of network data. The paper proposes an approach to detecting such attacks based on a combination of data mining methods, including machine learning models, and big data processing technologies. A methodology has been developed that includes algorithms for short-term and long-term event analysis implemented using two LSTM models. A modular architecture of the detection system has been built that takes into account the high load and the need to work in real time. The results of experimental testing have shown high accuracy (up to 99% / 82%  $f_1$  in binary / multi-class classification problems) and timeliness (30 sec. instant analysis / 7 days historical) of detecting attacks both in standard computer networks and in IoT environments.

**Keywords:** information security; multi-step attacks; machine learning; Big Data; LSTM; streaming data processing.

С развитием цифровых технологий информационные системы становятся все более сложными, что сопровождается ростом объема обрабатываемых данных и усложнением решаемых задач. В ответ на эти изменения как средства атаки, так и защитные механизмы непрерывно совершенствуются, адаптируясь к новым угрозам и условиям эксплуатации [1, 2].

Применяются различные подходы к проектированию систем защиты информации [3, 4]. Для обеспечения кибербезопасности применяются системы мониторинга, которые осуществляют постоянное наблюдение за состоянием сети, выявляют потенциальные угрозы и фиксируют инциденты, связанные с безопасностью [5, 6]. Передача информации о текущем состоянии защищаемой инфраструктуры осуществляется с помощью различных средств — от уведомлений до тревожных сигналов, информирующих о возможных или уже произошедших атаках.

Многошаговые атаки, реализуемые в несколько этапов [7], часто с участием различных злоумышленников и нацеленные на разные узлы сети, представляют собой одну из наиболее серьезных угроз информационной безопасности. Такие атаки сложно выявить с помощью традиционных систем обнаружения вторжений, поскольку они тщательно маскируются под легитимную сетевую активность.

Для эффективной защиты информационной инфраструктуры необходимо, чтобы системы безопасности могли оперативно идентифицировать критически важные события, в том числе многошаговые атаки, предоставлять исчерпывающую информацию о происходящем и прогнозировать возможные векторы дальнейшего распространения угроз [8].

С этой целью были разработаны различные методы обнаружения, включая подходы, основанные на технологиях машинного обучения. Тем не менее, с увеличением объемов поступающих данных и сложности анализа последовательных событий актуализируется проблема потоковой обработки информации в условиях

больших данных (Big Data, BD) [9], что требует новых решений в области быстродействующих и масштабируемых аналитических систем.

Разработка эффективных методов обнаружения сложных киберугроз представляет собой не просто задачу защиты отдельных информационных систем [10] — это ключевой аспект формирования доверия граждан к цифровой инфраструктуре и государственным онлайн-сервисам.

Актуальность данной проблемы усиливается в условиях стремительного роста объема передаваемой информации, необходимости её оперативной обработки и постоянно усложняющихся сценариев атак [11].

В связи с этим возрастает потребность во внедрении интеллектуальных и автоматизированных решений, основанных на машинном обучении и технологиях обработки больших данных [12]. Такие подходы позволяют не только своевременно зафиксировать факт вторжения, но и проводить поведенческий анализ действий злоумышленника [13], прогнозировать возможные шаги атаки и оперативно реагировать на угрозу, существенно снижая потенциальный ущерб и обеспечивая проактивную защиту критически важной цифровой инфраструктуры [14].

В рамках данной работы разработаны модели преобразования сетевых событий, позволяющие структурировать входной поток данных от защищаемых устройств путём их агрегации, упорядочивания и группировки в пакеты фиксированной длины.

Для обеспечения устойчивой обработки при нестабильном объёме входящих данных реализован механизм управления временным окном, позволяющий накапливать информацию и инициировать параллельную обработку с формированием независимых выборок.

Построена двухуровневая система обнаружения многошаговых атак: на первом уровне используется бинарный классификатор для выявления аномальных событий, на втором — модуль реконструкции атакующих сценариев с применением графовой модели взаимосвязей между событиями.

Для анализа полученных цепочек реализована модель многоклассовой классификации, ограниченная пространством допустимых сценариев, которое формируется на основе модели поведения потенциального нарушителя.

Разработаны алгоритмы, описывающие переход от необработанных событий к полному сценарию атаки, с учётом как краткосрочных, так и долгосрочных зависимостей между действиями злоумышленника. Все алгоритмы формализованы и адаптированы для внедрения в архитектуру систем обнаружения вторжений, с возможностью использования технологий машинного обучения и обработки больших данных.

В результате представлен подход, выявляющий как текущие атаки с ( $f_1 \geq 0.98$ ), так и длительные многошаговые сценарии ( $f_1 \geq 0.82$ ) с периодами 30 секунд и 7 дней соответственно. Представленный подход не теряет производительности при 100 эмулируемых потоках данных, а своевременность обнаружения при тестировании не превышает 6 секунд.

*Работа выполнена при частичной финансовой поддержке бюджетной темы FFZF-2025-0016.*

#### СПИСОК ЛИТЕРАТУРЫ

1. Kotenko I., Chechulin A., Novikova E. Attack Modelling and Security Evaluation for Security Information and Event Management // SECRIPT 2012 - Proceedings of the International Conference on Security and Cryptography. 2012. P.391-394. DOI: 10.5220/0004063403910394.
2. Komashinskiy D., Kotenko I. Malware detection by data mining techniques based on positionally dependent features // Proceedings of the 18th Euromicro Conference on Parallel, Distributed and Network-Based Processing, PDP 2010. Pisa, 2010. P.617-623. DOI: 10.1109/PDP.2010.30.
3. Desnitsky V., Levshun D., Chechulin A., Kotenko I. Design technique for secure embedded devices: application for creation of integrated cyber-physical security system // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications. 2016. Vol.7. № 2. P. 60-80. DOI: 10.22667/JOWUA.2016.06.31.060.
4. Десницкий В.А., Чечулин А.А., Котенко И.В., Левшун Д.С., Коломеец М.В. Комбинированная методика проектирования защищенных встроенных устройств на примере системы охраны периметра // Труды СПИИРАН. 2016. № 5 (48). С. 5-31. DOI: 10.15622/sp.48.1.
5. Branitskiy A., Kotenko I. Hybridization of computational intelligence methods for attack detection in computer networks // Journal of Computational Science. 2017. Vol.23. P.145-156. DOI: 10.1016/j.jocs.2016.07.010.
6. Schlenker A., Chowdhury A., Kiekintveld C., Laszka A., Vorobeychik Y. Don't bury your head in warnings: A game-theoretic approach for intelligent allocation of cyber-security alerts. 2017. <https://arxiv.org/abs/1706.06871>.
7. Moothedath S., Sinha A., Sen S., Bagchi S. A Game-Theoretic Approach for Dynamic Information Flow Tracking to Detect Multistage Advanced Persistent Threats // IEEE Transactions on Automatic Control. 2020. Т. 65, № 12. С. 5248–5263. DOI: 10.1109/TAC.2020.2976040.
8. Cisco. 2024 Global Networking Trends Report. Режим доступа: [https://www.cisco.com/c/dam/global/en\\_uk/solutions/enterprise-networks/2024-global-networking-trends.pdf](https://www.cisco.com/c/dam/global/en_uk/solutions/enterprise-networks/2024-global-networking-trends.pdf) [Электронный ресурс]. (дата обращения: 16.03.2025).
9. Trend Micro. TippingPoint Threat Protection System. Режим доступа: [https://www.trendmicro.com/en\\_us/business/products/network/intrusion-prevention/tipping-point-threatprotection-system.html](https://www.trendmicro.com/en_us/business/products/network/intrusion-prevention/tipping-point-threatprotection-system.html) [Электронный ресурс]. Дата обращения: 18.06.2023.
10. Cisco. Overview of Network Analysis and Intrusion Policies (Firepower v6.3). Режим доступа: [https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide/v63/overview\\_of\\_network\\_analysis\\_and\\_intrusion\\_policies.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide/v63/overview_of_network_analysis_and_intrusion_policies.html) [Электронный ресурс]. (дата обращения: 21.02.2025).
11. Broadcom. Security Center: Definitions Download (SEP 14). Режим доступа: <https://www.broadcom.com/support/security-center/definitions/download/detail?gid=sep14> [Электронный ресурс]. Дата обращения: 05.03.2022.
12. Kalosynakis M. D. Distributed Real-time Network Intrusion Detection System on Apache Spark: Thesis. Technical University of Crete, 2021.
13. Vassilev A. et al. Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations // NIST AI 100-2e2025. 2025. DOI: <https://doi.org/10.6028/NIST.AI.100-2e2025>.
14. Demetrio L., Coull S. E., Biggio B., Lagorio G., Armando A., Roli F. Adversarial EXEmples: A Survey and Experimental Evaluation of Practical Attacks on Machine Learning for Windows Malware Detection // ACM Transactions on Privacy and Security. 2021. Т. 24, № 4. Ст. 27. 31 с. DOI: <https://doi.org/10.1145/3473039>.

УДК 004

**ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОПЕРАЦИОННЫХ СИСТЕМ СЕМЕЙСТВА LINUX****Ивакина Мария Дмитриевна, Шилков Владимир Ильич**

Уральский федеральный университет имени первого Президента России Б. Н. Ельцина

Мира ул., 19, Екатеринбург, 620062, Россия

e-mails: mashaivakina26@gmail.com, vi.shilkov@urfu.ru

**Аннотация.** В статье обсуждаются вопросы применения инструментальных средств операционных систем на базе ядра Linux для решения задач в сфере информационной безопасности. Названы основные достоинства и недостатки операционной системы Linux. Приведены сведения об основных характеристиках инструментальных средств Linux для тестирования систем безопасности.

**Ключевые слова:** информационная безопасность; операционная система; тестирование безопасности.

**INFORMATION SECURITY TOOLS FOR LINUX FAMILY OPERATING SYSTEMS****Ivakina Maria, Shilkov Vladimir**

Ural Federal University named after the First President of Russia B. N. Yeltsin

19 Mira St, Yekaterinburg, 620062, Russia

e-mails: mashaivakina26@gmail.com, vi.shilkov@urfu.ru

**Abstract.** The article discusses the issues of using tools of operating systems based on the Linux kernel to solve problems in the field of information security. The main advantages and disadvantages of the Linux operating system are named. Information about the main characteristics of Linux security testing tools is provided.

**Keywords:** information security; operating system; security testing.

Эффективность информационно-коммуникационных технологий, систем и комплексов, применяемых для решения различных задач в промышленности, в бизнесе, в финансово-экономической сфере, зависит от большого количества факторов, к которым следует отнести, например, качество алгоритмов, вид языка программирования, квалификацию персонала, характеристики аппаратных средств. В значительной степени эффективность функционирования программно-аппаратных комплексов также зависит и от применяемой операционной системы, выбор которой зависит от возможностей и не всегда формализованных и обоснованных предпочтений пользователя.

Безусловным лидером на рынке операционных систем долгое время являлась операционная система Windows, разработанная корпорацией Microsoft и обладающая интуитивно понятным интерфейсом, совместимостью с различными видами программно-аппаратного обеспечения, безопасностью и многофункциональностью. Однако, в силу различных обстоятельств, связанных, в том числе и с уходом зарубежных компаний с российского рынка, возникла необходимость замены целого ряда программно-аппаратных средств, что во многом и обусловило выход на рынок свободно распространяемой операционной системы Linux. В контексте геополитических изменений и ухода международных компаний с российского рынка, выбор операционной системы становится стратегически важным решением для российских пользователей. Linux, как свободно распространяемая и открытая платформа, представляет собой жизнеспособную альтернативу коммерческим операционным системам.

Актуальность исследования вопросов, связанных с применением Linux, обусловлена, с одной стороны, растущей популярностью этой операционной системы, а с другой, наличием проблем, связанных с ее применением. Одной из таких проблем является проблема безопасности и, хотя Linux обладает значительными преимуществами в плане защиты, возникли новые риски, связанные с появлением множества вредоносных программ, специально созданных для Linux [1]. В соответствии со сведениями, приведенными в [2], система Linux имеет преимущества в безопасности в сравнении с операционными системами Windows и MacOS (операционная система для компьютеров Mac).

Более надежная безопасность по сравнению с проприетарными операционными системами достигается благодаря специальной архитектуре, гибкости настройки, разнообразию дистрибутивов, открытости исходного кода и активному развитию open-source инструментов. Вместе с тем следует отметить, что несмотря на то что благодаря открытости исходного кода, пользовательская аудитория выявляет и устраняет уязвимости, возникают риски безопасности, связанные с неправильной настройкой системы неподготовленными пользователями и действиями злоумышленников, создающих инструменты для взлома системы защиты.

Надежность Linux обеспечивается за счет реализации принципа минимальных привилегий, четкого распределения прав и строгого контроля за доступом. В системе существует три основных типа учетных записей, к которым относятся: пользователи (users) имеют ограниченные права, группы (groups) объединяют пользователей с общими разрешениями, суперпользователь с неограниченными правами (root), ошибки которого могут привести к катастрофическим последствиям [3]. Для проведения аудита информационной безопасности, выявления слабых мест и уязвимостей существует набор специализированных инструментов, входящих в дистрибутив операционной системы Kali Linux.

Особую ценность представляют специализированные дистрибутивы, которые включают мощные инструменты для тестирования безопасности: John the Ripper для анализа паролей, Aircrack-ng для аудита Wi-Fi сетей, Burp Suite для веб-приложений, Metasploit для работы с уязвимостями и Wireshark для анализа сетевого трафика. Эти инструменты, хотя и требуют профессиональных навыков, делают Linux исключительно эффективной платформой для обеспечения информационной безопасности [4].

Так, например, John the Ripper — программное средство, применяемое для тестирования стойкости паролей путем реализации атак методом перебора (brute-force) и с использованием предварительно вычисленных хешей (rainbow tables). Данная программа удобна для взлома паролей методом перебора, так как поддерживает более 260 форматов хешей (включая NTLM, Kerberos, MySQL) и позволяет гибко настраивать атаки (брутфорс, словарные атаки, гибридные методы). Однако у неё есть ряд недостатков, например: низкая эффективность против сложных алгоритмов, необходимость наличия высокопроизводительного оборудования для обеспечения достаточной скорости перебора, потребность в ручном составлении правил для словарей, что усложняет процесс [5].

Инструмент Burp Suite — это многофункциональная платформа для выявления уязвимостей в веб-приложениях, поддерживающая анализ трафика, работающего по протоколам HTTP/HTTPS, а также автоматизированное тестирование на наличие распространенных уязвимостей (например, SQL-инъекций, XSS).

Приложение Wireshark представляет собой широко распространенный сетевой анализатор, предназначен для захвата и анализа трафика сети и, который позволяет осуществлять перехват, детальный разбор и диагностику сетевого трафика в реальном времени. Приложение может взаимодействовать с наибольшим числом известных протоколов, имеет понятный графический интерфейс, а система фильтров позволяет сделать поиск более удобным.

Функционал Wireshark предоставляет следующие возможности: взаимодействие с большинством известных ОС, захват трафика в режиме «здесь и сейчас», возможность использовать множество встроенных дешифраторов протоколов, возможность сохранять и использовать ранее захваченный трафика сети, фильтрация и поиск пакетов по разным параметрам, выделение цветом пакетов разных протоколов, формирование статистики. Однако, несмотря на то что этот инструмент незаменим для анализа сетей, для его эффективного использования требуются определенные навыки [6].

Инструментальные средства Metasploit Framework образуют модульную платформу, предназначенную для разработки, тестирования и эксплуатации эксплойтов, что делает ее ключевым инструментом в процессе пентестирования. Инструменты содержат необходимую и нужную информацию для тех, кто занимается пополнением базы данных систем обнаружения атак (COA), а также изучением и анализом различных уязвимостей). Целью является сбор информации о таких слабых местах системы с кодами, которые их реализуют, чтобы сделать эту информацией доступной разработчикам и администраторам безопасности [7].

Каждый из рассмотренных инструментов обладает уникальными возможностями и применяется для решения специфических задач в области информационной безопасности. Их комбинация позволяет специалистам проводить комплексное тестирование и эффективно выявлять уязвимости в различных системах.

Таким образом, следует принять во внимание, что Linux не является абсолютно защищенным решением, так как злоумышленники, активно разрабатывают вредоносные программы для преодоления системы защиты. В связи с данным обстоятельством, разработка инструментов и методов повышения информационной безопасности информационных систем, разработанных на базе Linux, остается актуальной задачей. Вместе с тем, несмотря на наличие определенных рисков безопасности Linux является стабильной, безопасной и независимой операционной системой, так как архитектурные преимущества в сочетании с системой разграничения прав, минимальными привилегиями, открытость кода и мощными инструментами безопасности позволяют не только минимизировать риски, но и активно противодействовать киберугрозам.

В условиях цифровой трансформации переход на Linux может стать важным шагом к технологической независимости и информационной безопасности российской экономики. Однако, следует отметить, что для успешного внедрения и использования этой платформы требуются инвестиции в подготовку профессиональных специалистов и обучение пользователей.

#### СПИСОК ЛИТЕРАТУРЫ

1. Что такое операционная система Linux и насколько она безопасна? // Kaspersky URL: <https://www.kaspersky.ru/resource-center/definitions/linux> (Дата обращения 11.05.25)
2. Explore the Top Secure Linux Distro for Privacy & Security in 2025 // LinuxSecurity. 2025. URL: <https://linuxsecurity.com/features/explore-the-top-secure-linux-distro-for-privacy-security-in-2025> (дата обращения: 17.07.2025).
3. Основы безопасности в Linux // JavaRush URL: <https://javarus.com/quests/lectures/ru.javarush.system.linux.lecture.level05.lecture01> (Дата обращения 11.05.25)
4. Михейчик А. Д. Kali Linux в информационной безопасности //Инфокоммуникации: 55-я юбилейная конференция аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», 22-26 апреля 2019 г., БГУИР, Минск, Беларусь: тезисы докладов.—Мн.—2019.—104 с.; ил. 2019. С. 15.
5. John the Ripper: Password Cracking Tutorial and Review // eSecurity Planet URL: <https://www.esecurityplanet.com/products/john-the-ripper/> (Дата обращения 08.05.25)
6. Киреев А.П., Колмыков Д.В., Михайлов С.Ю., Пепеляев А.В. Анализ сетевого трафика корпоративной сети посредством программного обеспечения Wireshark //Фрактал. 2019. №. 3. С. 11-15.
7. Троицкий П. Исследование уязвимостей с помощью Metasploit Framework // Системный администратор. 2009. №. 1. С. 68-73.

УДК 004.056

**ПРОСТРАНСТВЕННАЯ КОНФИДЕНЦИАЛЬНОСТЬ: РИСКИ, МАСКИРОВАНИЕ  
И АРХИТЕКТУРА ДОВЕРИЯ ПРИ ОБРАБОТКЕ ГЕОДАННЫХ****Изотов Даниил Юрьевич, Яровой Роберт Владимирович**

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: daniil.izotov.1999@mail.ru, Nadzar@yandex.ru

**Аннотация.** В тезисе проанализированы риски, возникающие на этапах обращения с координатной информацией — от сбора до повторной идентификации, — а также представлены современные стратегии защиты: дифференциальная приватность, псевдонимизация, кластеризация маршрутов, локальная обработка.

**Ключевые слова:** геолокация; конфиденциальность; пространственные данные; деанонимизация; псевдонимизация; дифференциальная приватность; edge computing; приватность по умолчанию.

**SPATIAL PRIVACY: RISKS, MASKING AND TRUST ARCHITECTURE IN GEO DATA PROCESSING****Izotov Daniil, Yarovoy Robert**

Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: daniil.izotov.1999@mail.ru, Nadzar@yandex.ru

**Abstract.** The thesis analyzes the risks that arise at the stages of handling coordinate information — from collection to re-identification — and presents modern protection strategies: differential privacy, pseudonymization, route clustering, local processing.

**Keywords:** geolocation; privacy; spatial data; deanonymization; pseudonymization; differential privacy; edge computing; privacy by default.

Геоанные, изначально созданные для навигации, превратились в маркеры повседневной активности, позволяющие реконструировать цифровой силуэт субъекта. Точность координат, регулярность маршрутов и их поведенческая уникальность формируют основу для пространственного профилирования, предиктивной аналитики и вторичной идентификации [1].

Нарушение конфиденциальности происходит поэтапно — от фоново собираемых координат до их корреляции с демографическими и социальными источниками. Даже обезличенные данные не защищают от реидентификации, если сохраняется контекст: повторяемость маршрутов, синхронность с транзакциями, геотеги из соцсетей. Поведенческие паттерны (дом–работа–тренировка) становятся уникальными идентификаторами [2].

Современные угрозы выходят за рамки утечки: координатный след становится инструментом слежения, встраиваемым в экономику внимания и алгоритмы платформ. Конфиденциальность нарушается не в моменте, а структурно — через архитектуру данных.

Меры защиты подразделяются на технические и организационные. Среди технических практик выделяются механизмы  $\epsilon$ -дифференциальной приватности в формате geo-indistinguishability с добавлением стохастического шума, пространственно-временная агрегация, позволяющая снижать точность при сохранении аналитической значимости, а также кластеризация маршрутов с заменой координат на устойчивые к трассировке зоны [3].

Локальная обработка на устройствах минимизирует внешние риски. Однако эти решения страдают от закрытости, отсутствия масштабируемости и давления со стороны сервисов, чья эффективность зависит от точных данных [4].

Конфиденциальность требует архитектуры доверия, в которой алгоритмические, институциональные и пользовательские практики соединяются. Без осведомлённости субъектов, регулирующей среды и встроенных инженерных решений защита координат невозможна.

Таким образом, пространственная приватность — не вопрос сокрытия, а вопрос согласования интересов в условиях цифровой повседневности, где каждый шаг фиксируется, анализируется и возвращается к пользователю в виде персонализированного отклика.

**СПИСОК ЛИТЕРАТУРЫ**

1. Яровой Р.В., Рябов Г.А., Карганов В.В. Кибербезопасность в мире инфотелекоммуникаций: вызовы и стратегии защиты // Инновационная деятельность в Вооруженных Силах Российской Федерации. Труды всеармейской научно-практической конференции. Санкт-Петербург, 2023. С. 373-377.
2. Шурыгина К.И., Кокорева Е.В. Мобильное приложение для геолокации // Современные проблемы телекоммуникаций. материалы Всероссийской научно-технической конференции. Новосибирск, 2024. С. 261-264.
3. Черпаков И.В., Калинин М.И. Конфиденциальность данных в эпоху больших данных: проблемы и решения для предприятий // Социально-экономический ландшафт региона: развитие и логистические трансформации. Материалы Всероссийской научно-практической конференции преподавателей, студентов и практиков. Красноярск, 2024. С. 64-66.
4. Грязнов С.А. Проблемы с данными и конфиденциальностью в умных городах // Modern Science. 2021. № 1-2. С. 450-453.



УДК 004.056

## УЯЗВИМОСТИ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ: ВЕКТОРЫ АТАК И КОМПЛЕКСНЫЕ МЕРЫ ПРОТИВОДЕЙСТВИЯ

Клишин Александр Владимирович, Яровой Роберт Владимирович

Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: tms65xx@yandex.ru, Nadzar@yandex.ru

**Аннотация.** В тезисе систематизированы ключевые уязвимости, включая prompt injection, утечку обучающих данных, галлюцинации и отравление датасетов. Описаны подходы к анализу модели и представлена совокупность мер защиты. Подчеркнута необходимость комплексного контроля над жизненной цепочкой LLM.

**Ключевые слова:** большие языковые модели; LLM; уязвимости ИИ; prompt injection; защита модели; анализ безопасности; устойчивость модели; data poisoning; информационная безопасность.

## VULNERABILITIES OF LARGE LANGUAGE MODELS: ATTACK VECTORS AND COMPREHENSIVE COUNTERMEASURES

Klishin Alexander, Yarovoy Robert

Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: tms65xx@yandex.ru, Nadzar@yandex.ru

**Abstract.** The thesis systematizes key vulnerabilities, including prompt injection, training data leakage, hallucinations, and dataset poisoning. Approaches to model analysis are described and a set of protection measures is presented. The need for comprehensive control over the LLM life chain is emphasized.

**Keywords:** large language models; LLM; AI vulnerabilities; prompt injection; model protection; security analysis; model resilience; data poisoning; information security.

Интеграция больших языковых моделей в продуктивные ИТ-среды сопровождается не только ростом функциональных возможностей, но и обострением рисков, связанных с их уязвимостью. В отличие от классических программ, поведение LLM не запрограммировано явно, а формируется в результате обучения, что затрудняет предсказуемость и контроль [1].

Среди наиболее значимых угроз выделяются: prompt injection — подмена инструкций через текстовый ввод; утечки конфиденциальных данных — в форме непреднамеренного воспроизведения обучающего материала; галлюцинации — генерация вымышленных фактов с высокой убедительностью; атаки на обучающие выборки (data poisoning) — внедрение ложных паттернов; извлечение обучающих данных — через множественные запросы и анализ вероятностной генерации [2–4]. Данные векторы атак обостряются в условиях открытого пользовательского взаимодействия с LLM (чат-боты, ассистенты). В подобных сценариях модели становятся инструментом для обхода политик, генерации вредоносного кода, получения некорректных рекомендаций.

Методы противодействия охватывают несколько уровней: фильтрация и семантическая проверка входа предотвращают атаки на этапе запроса; усиление промптов (prompt hardening) обеспечивает жёсткое структурирование инструкции и роли модели; обучение с учётом уязвимостей включает атакующие сценарии в тренировочные выборки; ограничение генерации реализуется через блокировку запрещённых токенов, ограничение длины и фильтрацию по токсичности; архитектурные прокси-слои обеспечивают песочницы, модули оценки и разграничение доступа [1, 3].

Анализ поведения модели может проводиться как в чёрном ящике (через API и ввод), так и в белом (анализ внутренних слоёв и attention-матриц). Перспективным направлением выступает LLM-as-a-tester — использование одной модели для систематического аудита другой.

В совокупности, устойчивость LLM требует не локальных патчей, а проектирования целостной архитектуры безопасности: от отбора и очистки обучающих данных до автоматизированного контроля генерации на выходе. При этом каждый защитный механизм — лишь часть мозаики, которая требует постоянной адаптации к новым методам обхода.

## СПИСОК ЛИТЕРАТУРЫ

1. Зырянова И.Н., Чернавский А.С., Трубачев С.О. Prompt injection - проблема лингвистических уязвимостей больших языковых моделей на современном этапе // Научный результат. Вопросы теоретической и прикладной лингвистики. 2024. Т. 10. № 4. С. 40-52.
2. Яровой Р.В., Паращук И.Б. Взаимосвязь машинного зрения и информационной безопасности // В книге: Информационная безопасность регионов России (ИБРР-2023). XIII Санкт-Петербургская межрегиональная конференция. Материалы конференции. Санкт-Петербург, 2023. С. 178-180.
3. Попов А.А. Аудит и управление ответами нейросетей: стратегии борьбы с галлюцинациями больших языковых моделей // В сборнике: Язык. Культура. Общение. Материалы всероссийской научно-практической конференции. Санкт-Петербург, 2024. С. 281-283.
4. Герасименко Д.В., Намиот Д.Е. Извлечение тренировочных данных: риски и решения в контексте безопасности LLM // International Journal of Open Information Technologies. 2024. Т. 12. № 11. С. 9-19.

УДК 004.056

## ГЕНЕРАТИВНЫЕ МОДЕЛИ КАК ИНСТРУМЕНТ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ: УГРОЗЫ И КОНТРМЕРЫ

Клишин Александр Владимирович, Яровой Роберт Владимирович

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: tms65xx@yandex.ru, Nadzar@yandex.ru

**Аннотация.** В тезисе рассмотрены механизмы злоупотребления LLM в фишинге, имитации переписки, чатботах и генерации BEC-сценариев. Подчёркнута необходимость пересмотра стратегий защиты, усиления поведенческого анализа и применения самих моделей как средства противодействия угрозам.

**Ключевые слова:** социальная инженерия; LLM; киберугрозы; фишинг; искусственный интеллект; генеративные модели; защита информации; поведенческая безопасность; автоматизация атак.

## GENERATIVE MODELS AS A TOOL OF SOCIAL ENGINEERING: THREATS AND COUNTERMEASURES

Klishin Alexander, Yarovoy Robert

Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: tms65xx@yandex.ru, Nadzar@yandex.ru

**Abstract.** The thesis examines the mechanisms of LLM abuse in phishing, imitation of correspondence, chatbots and generation of BEC scenarios. The need to review defense strategies, strengthen behavioral analysis and use the models themselves as a means of countering threats is emphasized.

**Keywords:** social engineering; LLM; cyber threats; phishing; artificial intelligence; generative models; information security; behavioral security; automation of attacks.

Социальная инженерия как метод воздействия на поведенческие уязвимости человека трансформируется с приходом больших языковых моделей (LLM), которые обучены объёмных датасетах, способны воспроизводить тексты, неотличимые от человеческой речи, адаптируясь к лексике и стилю общения [1].

Классические фишинговые рассылки уступили место персонализированным атакам, с использованием LLM в автоматизированном режиме. Сценарии включают генерацию писем от имени технической поддержки, создание чатботов, имитирующих представителей организаций, а также воспроизведение стилистики корпоративной переписки в рамках атак типа BEC [2–3].

Вектор атаки строится по классической схеме: сбор открытых данных о жертве, формирование запроса к модели, генерация контента и передача через email, мессенджеры или подставные веб-интерфейсы. LLM добавляют в эту цепочку масштабируемость и скорость, лишая атакующего необходимости в ручной подготовке сообщений.

Традиционные средства защиты, ориентированные на шаблонность и формальные признаки (опечатки, странные адреса, общие формулировки), утрачивают эффективность. Новые тексты безупречно выверены, стилистически корректны и зачастую выстроены в логически непротиворечивые цепочки, затрудняя распознавание даже подготовленными сотрудниками [2].

Меры противодействия включают: адаптацию фильтров к новым выборкам, содержащим тексты, созданные LLM; поведенческий анализ коммуникации — с учётом временных зон, динамики ссылок и стилистических несоответствий; обязательное внедрение цифровых подписей и систем верификации легитимности писем; симуляции атак с применением LLM для обучения персонала; использование самих моделей для контр-анализа — выявления неестественно «гладких» текстов, проверки на соответствие корпоративному стилю, генерации реплайтов и семантической интерпретации [4].

Таким образом, LLM стали не только технологическим рывком в генерации текста, но и критическим фактором риска. Противодействие этим угрозам требует не пассивной защиты, а активного опережения — в области алгоритмов, психологии и организационных практик.

## СПИСОК ЛИТЕРАТУРЫ

- Осипенко А.Л. Технологии искусственного интеллекта в преступной деятельности: новые угрозы и вызовы // Общество и право. 2023. № 4 (86). С. 15–25.
- Аменицкий А.В., Рухович И.В., Аменицкая Л.А., Аменицкий Д.А. Кибербезопасность. Deep fake технологии // В сборнике: В мире науки и открытий. сборник статей Международного научно-исследовательского конкурса. Пенза, 2024. С. 26–31.
- Аменицкий А.В., Аменицкий Д.А. Кибербезопасность. Hacking AI // В сборнике: Научные исследования и разработки 2025. Сборник статей II Международной научно-практической конференции. Пенза, 2025. С. 39–47.
- Лукашенко В.И., Яровой Р.В. Роль искусственного интеллекта в информационной безопасности // В сборнике: Региональная информатика и информационная безопасность. Сборник трудов Санкт-Петербургской международной конференции и Санкт-Петербургской межрегиональной конференции. Санкт-Петербург, 2024. С. 121–124.

УДК 004.056

**ОБЕЗЛИЧИВАНИЕ ДАННЫХ В БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЯХ:  
ГРАНИЦЫ ПРИВАТНОСТИ**

**Клишин Александр Владимирович, Яровой Роберт Владимирович**  
Военная академия связи им. Маршала Советского Союза С. М. Буденного  
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия  
e-mails: tms65xx@yandex.ru, Nadzar@yandex.ru

**Аннотация.** В тезисе рассмотрены подходы к обезличиванию текстов с учётом лексико-семантических рисков, классификация техник трансформации, влияние на связность и когерентность данных. Подчёркнута необходимость гибридных решений, сочетающих защиту с сохранением аналитической пригодности.

**Ключевые слова:** обезличивание; анонимизация данных; языковые модели; утечка контекста; инструменты защиты данных; синтетические текстовые данные.

**DATA DE-PERSONALISATION IN BIG LANGUAGE MODELS:  
THE BOUNDARIES OF PRIVACY**

**Klishin Alexander, Yarovoy Robert**  
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny  
3 Tikhoretsky Av, St. Petersburg, 194064, Russia  
e-mails: tms65xx@yandex.ru, Nadzar@yandex.ru

**Abstract.** The thesis examines approaches to text depersonalization taking into account lexical and semantic risks, classification of transformation techniques, and impact on data coherence and coherence. The need for hybrid solutions that combine protection with preservation of analytical suitability is emphasized.

**Keywords:** depersonalization; data anonymization; language models; context leakage; data protection tools; synthetic text data.

Передача текстовых данных в языковые модели создаёт двойственное требование: сохранить значимость контекста и при этом исключить возможность идентификации субъекта. Простое удаление имён, телефонов и номеров оказывается неэффективным — современные модели способны реконструировать скрытые маркеры по стилю, лексике и тематике [1].

Классическое обезличивание удаляет явные идентификаторы, но не нарушает логики текста — и тем самым оставляет основу для ретроспективного восстановления. Анонимизация действует радикальнее, разрушая привязки к субъекту через обесцвечивание пространственно-временных координат, но часто ведёт к потере смысловой сцепки. Псевдонимизация, будучи компромиссом, допускает восстановление исходного вида при наличии ключей, но уязвима при утечке инфраструктуры [2]. Особую угрозу представляет феномен контекстной деанонимизации, при котором текст, даже очищенный от явных следов, может быть соотнесён с внешними источниками — от социальных сетей до баз утечек — за счёт латентных паттернов речи, профессиональной терминологии и частотных распределений. Устранение этого риска требует не технического удаления, а стилистической и структурной трансформации.

Ключевые техники защиты включают: контекстную замену именных групп с использованием NER и генерацией структурно схожих сущностей; лингвистическую перестройку, модифицирующую синтаксические и морфологические паттерны; применение моделей для создания квазиреалистичных, но безопасных текстов при сохранении функциональной когерентности.

Наиболее продвинутые подходы опираются на дифференциальную приватность, вводящую шум в параметры fine-tuning или ограничивающую чувствительность градиентов. Однако прямое применение таких методов к текстам приводит к нарушению связности, особенно в задачах, где требуется извлечение смыслов, аннотирование и тематическое обобщение [3].

Сложность в том, что защита достигается ценой когнитивной обеднённости. Избыточная фильтрация приводит к «переанонимизации» — обнулению семантики при сохранении формального уровня безопасности. Ошибочная маркировка фрагментов как «чувствительных» может лишить LLM критического контекста, тогда как пропущенные уязвимости могут привести к компрометации. Следовательно, анонимизация в эпоху LLM — не утилитарная операция, а процесс интеллектуального баланса между статистикой, смыслом и этикой. Без понимания механизмов невозможно выстроить устойчивую архитектуру защиты.

**СПИСОК ЛИТЕРАТУРЫ**

1. Анесбай М.Е. Исследование моделей и алгоритмов проектирования информационной системы с обезличиванием персональных данных // Новые научные исследования : сборник статей VII Международной научно-практической конференции. Пенза, 2022. С. 56-59.
2. Волокитина Е.С. Алгоритмы анонимизации базы данных, содержащей персональные данные // В мире научных открытий. 2012. № 8 (32). С. 22-37.
3. Аскерова И.Р. Методы защиты конфиденциальности больших данных // В сборнике: МОЛОДЕЖЬ И СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ. Сборник трудов XVIII Международной научно-практической конференции студентов, аспирантов и молодых ученых. Томск, 2021. С. 358-359.

УДК 004.492.3

**ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ОБНАРУЖЕНИЯ АНОМАЛИЙ В ВЕБ-ТРАФИКЕ****Колинко Инна Павловна**

СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия

e-mail: kiina131313@gmail.com

**Аннотация.** В работе анализируются современные методы обнаружения аномалий в веб-трафике с применением ИИ. Распространение трафика с шифрованием, рост числа атак с использованием легитимных инструментов, а также опасность атак «нулевого дня», подчёркивает актуальность внедрения систем защиты на основе ИИ. Обученные на нормальном трафике, эти системы выявляют аномалии, предотвращая вторжение злоумышленников. В ходе исследования был проведен анализ работ, предложены общие принципы проектирования систем обнаружения вторжений на основе ИИ. Обобщены подходы к разработке архитектур на базе ИИ, способы подготовки данных и методы отбора релевантных признаков. Выделены тенденции к разработке универсальных и объяснимых систем обнаружения вторжений COB, сочетающим пространственно-временной анализ трафика и поиск скрытых закономерностей в данных.

**Ключевые слова:** веб-трафик; обнаружение аномалий; системы обнаружения вторжений (COB).

**AI-BASED APPROACHES TO ANOMALY DETECTION IN WEB TRAFFIC****Kolinko Inna**

St. Petersburg Federal Research Center of the Russian Academy of Sciences

39 14th Line VO, St. Petersburg, 199178, Russia

e-mail: kiina131313@gmail.com

**Abstract.** This study analyzes contemporary methods of anomaly detection in web traffic using artificial intelligence (AI). The increasing prevalence of encrypted traffic, the rise in attacks leveraging legitimate tools, and the growing threat of zero-day exploits underscore the importance of implementing AI-based defense systems. Trained on patterns of normal traffic, such systems can detect anomalies and prevent unauthorized intrusions. The research includes an analysis of existing studies and proposes general principles for designing AI-driven intrusion detection systems. It summarizes approaches to the development of AI-based architectures, data preprocessing techniques, and methods for selecting relevant features. Furthermore, it highlights current trends toward developing universal and explainable intrusion detection systems (IDS) that integrate spatiotemporal traffic analysis with the identification of hidden data patterns.

**Keywords:** web traffic; anomaly detection; IDS.

Современные исследования в области систем обнаружения вторжений (COB), основанных на методах искусственного интеллекта, ориентированы на повышение точности, универсальности и объяснимости. Одним из ключевых направлений является развитие гибридных архитектур, которые совмещают преимущества различных моделей глубокого обучения. В таких системах используются сверточные нейронные сети (CNN) для извлечения локальных признаков, рекуррентные архитектуры LSTM и GRU для анализа временных зависимостей, а также автоэнкодеры для снижения размерности и выявления аномалий. Комбинация этих методов позволяет учитывать пространственные и временные характеристики сетевого трафика, что делает возможным обнаружение сложных атак. Так, архитектура CNN+LSTM [1] показала точность 98,85% на датасете UNSW-NB15, а также продемонстрировала высокую производительность на устройствах с ограниченными вычислительными ресурсами.

Особый интерес вызывают мультимодальные автоэнкодеры, способные интегрировать информацию из различных источников. В работе [2] предложено решение, где MDAE используется совместно с GRU и эвристическим алгоритмом Tuna Swarm Optimization (TSO). Этот подход продемонстрировал точность 99,1% на CICIDS2017 при минимальном уровне ложных срабатываний. Преимуществом данного метода является не только высокая точность, но и возможность сокращения числа используемых признаков, что снижает нагрузку на систему и повышает её производительность. Автоэнкодеры также успешно применяются в задаче выявления аномалий: модель, объединяющая автоэнкодер с методами OCSVM и гауссовых смесей, показала точность 98,73% на NSL-KDD [3], хотя ограничением остаётся устаревший характер используемого набора данных.

Существенным направлением развития IDS является анализ содержимого пакетов (payload-based analysis). Традиционные системы ограничиваются обработкой заголовков, однако современные атаки, включая SQL- и HTTP-инъекции, требуют анализа полезной нагрузки. Для решения этой задачи предложены методы векторизации, вдохновлённые обработкой естественного языка. В исследовании [4] применён модифицированный алгоритм Word2Vec для преобразования байтовых последовательностей в векторные представления, а классификация осуществлялась с помощью k-ближайших соседей. На наборах данных CICIDS2017 и STU-13 данный метод достиг точности 99%, что свидетельствует о его эффективности при обнаружении атак на прикладном уровне. В то же время подобные решения сталкиваются с проблемами

масштабируемости и высокой вычислительной сложности, особенно при анализе потокового трафика в реальном времени.

Не менее важным направлением остаётся оптимизация признакового пространства. Высокая размерность сетевых данных существенно усложняет задачу классификации и увеличивает нагрузку на IDS. Эвристический алгоритм TSO (Tuna Swarm Optimization) [2], обеспечивает эффективный выбор признаков и демонстрирует универсальность для различных типов трафика. Альтернативный подход — гибридный отбор признаков (HFS) — сочетает методы корреляционного анализа и рекурсивного исключения признаков. Его использование в связке с LightGBM позволило достичь точности 98,72% на NSL-KDD [5], а также обеспечить высокую производительность при обработке потоковых данных, что является критически важным для практических IDS.

Сравнительный анализ представленных решений показывает, что гибридные модели обеспечивают наилучший баланс точности и универсальности. CNN+LSTM [1] отличается применимостью в условиях ограниченных ресурсов, TSO+MDAE+GRU [2] демонстрирует высокую адаптивность к современным атакам, автоэнкодеры с OCSVM [3] эффективны для задач поиска аномалий, а payload-анализ [4] и гибридный отбор признаков [5] обеспечивают высокий уровень выявления атак на прикладном уровне.

Однако практическое внедрение интеллектуальных СОВ сталкивается с рядом нерешённых задач. Во-первых, масштабируемость и способность систем функционировать в условиях реального времени остаются ограниченными из-за сложности обработки больших объёмов сетевого трафика. Во-вторых, интерпретируемость выводов моделей является критическим фактором, так как специалисты по информационной безопасности нуждаются в понимании причин, по которым система классифицировала событие как аномальное. Недостаток прозрачности решений затрудняет расследование инцидентов и снижает доверие к системам.

В перспективе исследования будут сосредоточены на разработке моделей, методик и алгоритмов для СОВ, которые одновременно обеспечивают высокую вычислительную эффективность и объяснимость решений. Такие системы станут ключевым элементом защиты от атак «нулевого дня» и будут способствовать повышению устойчивости цифровой инфраструктуры в условиях роста сложности и изощрённости киберугроз.

#### СПИСОК ЛИТЕРАТУРЫ

1. Altaie R.H., Hoomod H.K. An Intrusion Detection System using a Hybrid Lightweight Deep Learning Algorithm // Engineering, Technology & Applied Science Research. 2024. Vol. 14, No. 5. P. 16740–16743. DOI: 10.48084/etasr.7657.
2. Gowthami G., Silvia Priscila S. Tuna swarm optimisation-based feature selection and deep multimodal-sequential-hierarchical progressive network for network intrusion detection approach // International Journal of Computational Complexity and Biomedical Systems. 2024. 30 Jan. P. 355–374. DOI: 10.1504/IJCCBS.2023.136338.
3. Wang C., Sun Y., Lv S., Wang C., Liu H., Wang B. Intrusion Detection System Based on One-Class Support Vector Machine and Gaussian Mixture Model // Electronics. 2023. Vol. 12. Article No. 930. DOI: 10.3390/electronics12040930.
4. Mehedi Hassan, Md Enamul Haque, Mehmet Engin Tozal, et al. Intrusion Detection Using Payload Embeddings // IEEE Access. 2021. Received: October 25; accepted: December 1; published: December 30; current version: January 13, 2022. DOI: 10.1109/ACCESS.2021.3139835.
5. Logeswari G., Bose S., Thangasamy Anitha. An Intrusion Detection System for SDN Using Machine Learning // Intelligent Automation & Soft Computing. 2023. Vol. 35. P. 867–880. DOI: 10.32604/iasc.2023.026769.

УДК 003.26

#### МЕТОД ПОВЫШЕНИЯ ПРОИЗВОДИТЕЛЬНОСТИ АЛГЕБРАИЧЕСКИХ АЛГОРИТМОВ ЭЦП СО СКРЫТОЙ ГРУППОЙ

Костина Анна Александровна

СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия

e-mail: to.ann@inbox.ru

**Аннотация.** Алгебраические алгоритмы ЭЦП, стойкость которых основана на вычислительной трудности решения систем степенных уравнений с многими переменными, представляют интерес как практические постквантовые криптосхемы. В качестве алгебраического носителя в них используются конечные некоммутативные ассоциативные алгебры (КНАА) с глобальной двухсторонней единицей, умножение в которых задается по таблицам умножения базисных векторов (ТУБВ). Для повышения производительности указанных алгоритмов используются КНАА, заданные по прореженным ТУБВ, однако последние известны только для случая четырехмерных КНАА, хотя для получения 256-битной стойкости предпочтительным является использование КНАА более высоких размерностей. С целью задания многомерных КНАА по ТУБВ с большим числом ячеек, включающих нулевую структурную константу, предложено использовать недавно предложенный метод вложения, в котором некоторая известная ТУБВ встраивается в другую известную с сохранением свойства ассоциативности операции умножения векторов. Предлагаемый способ состоит в использовании одной или обеих ТУБВ прореженного типа. Таким способом построен ряд прореженных ТУБВ для задания восьмимерных и шестнадцатимерных КНАА. Для первых достигнуто снижение вычислительной сложности операции умножения в два раза, а для вторых — в четыре раза по сравнению со случаем «плотных» ТУБВ такой же размерности.

**Ключевые слова:** компьютерная безопасность; постквантовая криптография; алгоритмы цифровой подписи; конечные алгебры; ассоциативные алгебры; некоммутативные алгебры.

## A METHOD FOR INCREASING THE PERFORMANCE OF ALGEBRAIC SIGNATURE ALGORITHMS WITH A HIDDEN GROUP

Kostina Anna

St. Petersburg Federal Research Center of the Russian Academy of Sciences

39 14-th Linia, VI, St. Petersburg, 199178, Russia

e-mail: to.ann@inbox.ru

**Abstract.** Algebraic signature algorithms, the security of which is based on the computational difficulty of solving the systems of power equations with many variables, are of interest as practical postquantum cryptoschemes. As an algebraic carrier, they use finite non-commutative associative algebras (FNAA) with a global two-sided unit, multiplication in which is set by the tables of multiplication of basic vectors (TMBV). To increase the performance of these algorithms, FNAA specified by sparse TMBV are used, however, the latter are known only for the case of four-dimensional FNAA, although the use of higher dimensions is preferable to obtain 256-bit security. In order to set the multidimensional FNAA by TMBV with a large number of cells, including zero structural constant, it is proposed to use the recently proposed imbedding method, in which some well-known TMBV is embedded into another one, preserving the property of association of the operation of the multiplication of the vectors. The proposed method consists in the use of one or both TMBV of the sparse type. In this way, a number of sparse TMBV were built for setting eight-dimensional and sixteen-dimensional FNAA. For the former (latter) FNAA, the two (four) times decrease in computational complexity of the multiplication operation was achieved compared to the case of “dense” TMBV of the same dimension.

**Keywords:** computer security; postquantum cryptography; digital signature algorithms; finite algebras; associative algebras; non-commutative algebras.

Интерес к алгебраическим алгоритмам электронной цифровой подписи (ЭЦП) [1, 2], стойкость которых базируется на вычислительной трудности решения больших систем степенных уравнений, обусловлена тем, что квантовый компьютер не является эффективным для их взлома, т.е. алгоритмы данного типа являются постквантовыми [3]. Существенным с практической точки зрения является то, что размеры открытого ключа и подписи в них являются существенно меньшими по сравнению с многими известными постквантовыми алгоритмами ЭЦП. В качестве алгебраического носителя в первых используются конечные некоммутативные ассоциативные алгебры (КНАА) с глобальной двухсторонней единицей, заданные над конечными полями четной [4] или нечетной [1] характеристики. Операция умножения в КНАА определяется по так называемым таблицам умножения базисных векторов (ТУБВ) [5]. В общем случае для реализации умножения в  $m$ -мерной КНАА требуется выполнить  $m \times m$  умножений в базовом конечном поле, связанных с попарным перемножением координат векторов-сомножителей, и примерно столько же сложений.

Также в ТУБВ используются структурные константы, вносящие дополнительные операции умножения в базовом поле, однако умножения на структурные константы и сложения вносят сравнительно малый вклад в вычислительную сложность операции векторного умножения, поэтому верхнюю границу последней можно оценить как  $m \times m$  умножений в базовом поле.

Если в ТУБВ присутствует  $n$  ячеек, содержащих структурную константу, равную нулю, то сложность векторного умножения составит  $m \times m - n$  умножений в базовом поле. Прореженными называются ТУБВ с ячейками, содержащими нулевую структурную константу. Степенью прореженности ТУБВ будем называть долю ячеек, содержащих нулевую структурную константу, а размерностью ТУБВ – размерность КНАА, для которой задается операция умножения. Известны четырехмерные КНАА со степенью прореженности 50%, задаваемые по прореженным ТУБВ с восемью ячейками с нулевой структурной константой [6].

Использование в качестве алгебраического носителя прореженных ТУБВ является одним из приемов повышения производительности алгоритмов ЭЦП на КНАА [7].

Однако, известные алгоритмы ЭЦП на четырехмерных ТУБВ обеспечивают уровень от 80-битной до 128-битной стойкости и для повышения стойкости до 256-битного уровня является актуальным использование КНАА с размерностью от  $m = 6$  до  $m = 16$ . При этом для таких размерностей в литературе предложены способы унифицированного задания КНАА произвольных четных размерностей  $m > 4$ , но неизвестны прореженные ТУБВ.

В данной работе рассматривается вопрос построения прореженных ТУБВ для задания многомерных КНАА с вычислительно эффективной операцией умножения. Для реализации таких ТУБВ предлагается использовать метод вложения, описанный в работе [8] и применить его для случая прореженных исходных ТУБВ.

Предлагаемый способ позволяет реализовать следующие варианты многомерных прореженных ТУБВ, задающих ассоциативное и некоммутативное умножение векторов:

1. Вложение прореженной четырехмерной ТУБВ в двухмерную ТУБВ обеспечивает построение восьмимерных ТУБВ со степенью прореженностью 50%.
2. Вложение двухмерной ТУБВ в прореженную четырехмерную ТУБВ обеспечивает построение восьмимерных ТУБВ со степенью прореженностью 50%.
3. Вложение прореженной четырехмерной ТУБВ в «плотную» четырехмерную ТУБВ обеспечивает построение шестнадцатимерных ТУБВ со степенью прореженностью 50%.
4. Вложение «плотной» четырехмерной ТУБВ в прореженную четырехмерную ТУБВ обеспечивает построение шестнадцатимерных ТУБВ со степенью прореженностью 50%.

5. Вложение прореженной четырехмерной ТУБВ в прореженную четырехмерную ТУБВ обеспечивает построение шестнадцатимерных ТУБВ со степенью прореженности 75%.

Для последнего варианта для фиксированного базового конечного поля обеспечивается четырехкратный выигрыш в эффективности операции умножения в КНАА по сравнению со случаем задания шестнадцатимерных КНАА по «плотным» ТУБВ.

С учетом того, что с ростом размерности КНАА могут использоваться базовые конечные поля, в которых порядок имеет существенно меньшую разрядность, реализация известных алгебраических схем ЭЦП [2, 7, 9] на 16-мерных прореженных КНАА потенциально обеспечивает повышение уровня стойкости при сохранении высокой производительности.

Для повышения производительности и уменьшения схемотехнической сложности аппаратной реализации алгебраических алгоритмов ЭЦП со скрытой группой представляет интерес использование КНАА, заданных над конечными полями четного порядка по прореженным ТУБВ.

*Работа поддержана грантом РНФ № 24-21-00225, <https://rscf.ru/project/24-21-00225/>.*

#### СПИСОК ЛИТЕРАТУРЫ

1. Молдован Д.Н., Молдован А.А. Алгебраические алгоритмы ЭЦП, основанные на трудности решения систем уравнений // Вопросы кибербезопасности. 2022. № 2(48). С. 7–17. DOI: 10.21681/2311-3456-2022-2-7-17.
2. Moldovyan A.A., Moldovyan N.A. A method for enhancing randomization in algebraic signature algorithms on non-commutative algebras // Quasigroups and related systems. 2025. V. 33. N. 1. P. 71–83. DOI: 10.56415/qrs.v33.06.
3. Ding J., Petzoldt A. Current State of Multivariate Cryptography // IEEE Security and Privacy Magazine. 2017. V. 15. N. 4. P. 28–36.
4. Молдован А.А., Молдован Н.А. Алгоритмы ЭЦП на конечных некоммутативных алгебрах над полями характеристики два // Вопросы кибербезопасности. 2022. № 3(49). С. 58–68. DOI: 10.21681/2311-3456-2022-3-58-68.
5. Moldovyan N.A. Unified Method for Defining Finite Associative Algebras of Arbitrary Even Dimensions // Quasigroups and related systems. 2018. V. 26. N. 2. P. 263–270.
6. Moldovyan D.N., Moldovyan A.A., Moldovyan N.A. Structure of a finite non-commutative algebra set by a sparse multiplication table // Quasigroups and related systems. 2022. V. 30. N. 1. P. 133–140. DOI: 10.56415/qrs.v30.11.
7. Молдован Н.А., Петренко А.С. Алгебраический алгоритм ЭЦП с двумя скрытыми группами // Вопросы кибербезопасности. 2024. № 6(64). С. 98–107. DOI: 10.21681/2311-3456-2024-6-98-107.
8. Dinh K.-L., Nguyen L.-G., Do T.-B., Moldovyan A.A., Moldovyan D.N., Kostina A.A. Defining high-dimensional non-commutative algebras as carriers for post-quantum digital signature algorithms // Proc. of the 1st International Conference on cryptography and information security (VCRIS). Hanoi, Vietnam, 2024. P. 1–5. DOI: 10.1109/VCRIS63677.2024.10813386.
9. Duong M.T., Moldovyan A.A., Moldovyan D.N., Nguyen M.H., Do T.-B. Structure of quaternion-type algebras and a post-quantum signature algorithm // International Journal of Electrical and Computer Engineering (IJECE). 2024. V. 15. № 3. P. 2965–2976. DOI: 10.11591/ijece.v15i3.pp2965-2976.

УДК 004.056

#### МЕТОДОЛОГИЯ ПОВЫШЕНИЯ ЗАЩИЩЕННОСТИ РАСПРЕДЕЛЕННОГО РЕЕСТРА СИСТЕМ УМНОГО ГОРОДА

**Крундышев Василий Михайлович, Калинин Максим Олегович**  
Санкт-Петербургский политехнический университет Петра Великого  
Политехническая ул., 29, Санкт-Петербург, 195251, Россия  
emails: vmk@ibks.spbstu.ru, max@ibks.spbstu.ru

**Аннотация.** Статья посвящена проблеме обеспечения защищенности распределенного реестра, используемого при создании цифровых инфраструктур умного города. Для защиты от атак, направленных на деанонимизацию участников сети и изменение истории транзакций, а также для обеспечения высокой производительности распределенного реестра разработан комплекс методов, базирующихся на принципах чесночной маршрутизации, модели доверия и механизме распределенного консенсуса.

**Ключевые слова:** блокчейн; модель доверия; распределенный консенсус; умный город; чесночная маршрутизация.

#### METHODOLOGY FOR INCREASING THE SECURITY OF THE DISTRIBUTED LEDGER OF SMART CITY SYSTEMS

**Krundyshov Vasiliy, Kalinin Maxim**  
Peter the Great St. Petersburg Polytechnic University  
29 Polytechnicheskaya St, St. Petersburg, 195251, Russia  
e-mails: vmk@ibks.spbstu.ru, max@ibks.spbstu.ru

**Abstract.** The paper is devoted to the problem of ensuring the security of a distributed ledgers used in the creation of digital infrastructures of a smart city. To protect against attacks aimed at deanonymizing network participants and changing transaction history, as well as to ensure high performance of the distributed registry, a set of methods based on the principles of garlic routing, a trust model, and a distributed consensus mechanism has been developed.

**Keywords:** blockchain; trust model; distributed consensus; smart city; garlic routing.

Технология распределенных реестров данных (distributed ledger technology, DLT) успешно применяемая в банковской сфере при создании платежных систем, становится одним из драйверов цифровизации и устойчивого развития новых мегаполисов [1]. Распределенный реестр может использоваться для повышения прозрачности, безопасности и эффективности различных процессов, включая управление финансовыми и нефинансовыми активами, контроль за цепочками поставок, управление большими данными, а также создание цифровых систем типа «безопасный город» [2, 3]. Однако, при использовании данной технологии в самоорганизующихся и неоднородных инфраструктурах умного города возникает ряд проблем:

- обеспечение анонимности. За счет выявления закономерностей в сетевом трафике, анализа временных меток и последовательности передачи сетевых пакетов злоумышленник может определить узлы, участвующие в цепочке транзакций, а также установить связи между участниками распределенного реестра умного города;

- обеспечение византийской отказоустойчивости. Захватив контроль над слаботзащищенными устройствами умного города, злоумышленник может обойти механизм консенсуса в распределенном реестре и выполнить вредоносные действия, например, изменить историю транзакций, препятствовать подтверждению новых транзакций;

- обеспечение высокой производительности. Для крупномасштабных сред умного города с большим количеством участников, узлов и защищаемых данных необходимо использовать алгоритмы, обеспечивающие высокую скорость обработки большого количества транзакций.

Для защиты от атак, направленных на деанонимизацию пользователей, разработан метод анонимизации сетевого трафика, базирующийся на применении принципов честной маршрутизации. Сохранение согласованности данных, поддержка интеграции с механизмами консенсуса, взаимодействие узлов с использованием настроенных таблиц маршрутизации позволяют обеспечить конфиденциальность и прозрачность. Для повышения защищенности распределенного реестра от атак, связанных с подделкой транзакций, предложен метод на основе модели доверия, которая наделяет каждого участника динамическим весом голоса, зависящим от истории его корректного или некорректного поведения. Новый механизм позволяет выявлять и изолировать вредоносные узлы на ранних этапах работы сети, снижая их влияние на процесс голосования и тем самым повышая византийскую отказоустойчивость распределенного реестра, а также общую надежность всей системы. Для повышения производительности распределенного реестра систем умного города разработан новый алгоритм распределенного консенсуса, основанный на агрегации алгоритмов Tangle и Proof-of-Authority, защищенный с помощью технологий доверенных вычислений и удаленной аттестации. Предложенное решение обеспечивает безопасность блокчейна, компенсируя изъяны базовых алгоритмов распределенного консенсуса; универсальность и высокую производительность при обработке большого числа транзакций.

В результате анализа научно-технических источников, посвященных созданию решений, направленных на повышение защищенности распределенного реестра в системах умного города, установлено, что на сегодняшний день существует ряд проблем, связанных с обеспечением безопасности и высокой производительности. В данном исследовании для решения перечисленных проблем предложен комплекс методов, разработанных с учетом специфики функционирования цифровых инфраструктур умного города.

*Исследование выполнено за счет гранта Российского научного фонда №24-11-20005, <https://rscf.ru/project/24-11-20005/>, грант Санкт-Петербургского научного фонда (Соглашение №24-11-20005 о предоставлении регионального гранта).*

## СПИСОК ЛИТЕРАТУРЫ

1. Кузнецов А. М. Методы верификации данных в умных городах на стыке искусственного интеллекта распределенных реестров и сетевой теории // Академический исследовательский журнал. 2023. Т. 1. №. 1. С. 8-19.
2. Петренко С. А., Балябин А. А. Модель квантовых угроз безопасности информации для национальных блокчейн-экосистем и платформ // Вопросы кибербезопасности. 2025. №. 1 (65). С. 7-17.
3. Донсков Е. А., Котенко И. В. Подходы к обнаружению атак на слой блокчейна в интеллектуальных транспортных сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании. 2024. С. 292-296.

УДК 004.5

## СВЕДЕНИЕ ЗАДАЧИ ПРОЕКТИРОВАНИЕ ГРАФИЧЕСКИХ ИНТЕРФЕЙСОВ К ОПТИМИЗАЦИОННОЙ

**Курта Павел Александрович<sup>1</sup>, Израйлов Константин Евгеньевич<sup>2</sup>**

<sup>1</sup> ООО «Норд клининг»

Героев-Североморцев пр., 11, корп. 2, пом. 2а/1-8, Мурманск, 183031, Россия

<sup>2</sup> СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия

e-mails: [expert@kurta.ru](mailto:expert@kurta.ru), [konstantin.izrailov@mail.ru](mailto:konstantin.izrailov@mail.ru)

**Аннотация.** Рассматриваются задача проектирования эффективных интерфейсов взаимодействия пользователя с информационной системой, которая сводится к комбинаторной оптимизации; при этом, целевой функцией является эффективность интерфейса, а параметрами — типы и расположение его элементов.



**Ключевые слова:** информационная система; интерфейс; эффективность; комбинаторная оптимизация; графические формы.

## REDUCING THE PROBLEM OF DESIGNING GRAPHIC INTERFACES TO OPTIMIZATION

Kurt Pavel<sup>1</sup>, Izrailov Konstantin<sup>2</sup>

<sup>1</sup> ООО «Nord cleaning»

Geroev-Severomortsev Ave., 11, bldg. 2, room 2a/1-8, Murmansk, 183031, Russia

<sup>2</sup> St. Petersburg Federal Research Center of the Russian Academy of Sciences

39 14th Line VO, St. Petersburg, 199178, Russia

e-mails: expert@kurta.ru, konstantin.izrailov@mail.ru

**Abstract.** The problem of designing effective interfaces for user interaction with an information system is considered, which is reduced to combinatorial optimization; in this case, the objective function is the efficiency of the interface, and the parameters are the types and location of its elements.

**Keywords:** information system; interface; efficiency; combinatorial optimization; graphic forms.

Интеграция информационных технологий в жизнь современного общества актуализировала различные аспекты взаимодействия с данными, одними из которых стали интерфейсы информационных систем. При этом, успешность пользования услугами таких систем напрямую зависит и от эффективности применяемых интерфейсов (в преобладающем большинстве — графических) [1], под которой авторы понимаю следующие показатели (и способы их вычисления) [2]:

- результативность — степень безошибочного ввода (и вывода) данных,
- оперативность — скорость такого ввода, и
- ресурсо-экономность — обратный показатель от психо-эмоциональной нагрузки пользователя при работе с данными.

Необходимо отметить, что такая интерпретация показателей более подходит для отдельного класса интерфейсов, характерных для информационных систем запросного типа — когда пользователю необходимо получить информацию из базы данных (возможно с пред- или постобработкой). Указанная эффективность может вычисляться, как интегральная от элементов интерфейсов — графических форм, полей ввода/вывода и др.; при этом, она зависит от обрабатываемых данных.

Повышения эффективности интерфейсов достигается их продуманным проектированием, что с точки зрения системного анализа может быть сведено к решению оптимизационной задачи по комбинированию форм и их элементов [3]. Так, целевой функцией считается итоговая эффективность, декомпозируемая на эффективности отдельных элементов; оптимизируемыми же параметрами являются типы графических элементов, их расположение на формах, а также сама «разбивка» форм.

Представление эффективности в аналитическом виде [4], как и зависимость эффективности элементов от обрабатываемых данных (названная атомарной) были получены ранее [5].

Таким образом, на данном этапе исследования требуется создание метода (точнее, алгоритма) оптимизации, а также, архитектуры соответствующей системы и ее программной реализации. Как следствие, современные интерфейсы смогут перейти в разряд динамических, подстраиваемых под конкретные обрабатываемые данные и потребности пользователей — путем установки соответствующих весовых коэффициентов для показателей эффективности.

Для решения такого рода оптимизационных задач существует целый набор методов, среди которых (помимо очевидного перебора) отдельно можно выделить эвристические, а именно, следующие алгоритмы:

- жадный,
- локальный поиск,
- отжиг,
- генетический,
- поиск с запретами,
- муравьиный и
- алгоритм роя частиц.

Предварительно сложно предсказать, какой из алгоритмов окажется более «удачным» для решения указанной оптимизационной задачи, что очевидно потребует их как качественного (теоретического), так и количественного (практического) сравнения.

## СПИСОК ЛИТЕРАТУРЫ

1. Курта П.А., Коломеев М.В. Обобщенная классификация интерфейсов транспортной инфраструктуры «Умного города» // Вестник кибернетики. 2020. № 4(40). С. 6-13. DOI 10.34822/1999-7604-2020-4-6-13.
2. Курта П.А. Взаимодействие пользователя с информационной системой. Часть 3. Оценка эффективности // Известия СПбГЭТУ ЛЭТИ. 2021. № 4. С. 58-72.
3. Левин М.Ш. Комбинаторная оптимизация при построении конфигураций систем // Информационные процессы. 2008. Т. 8. № 4. С. 256-300.
4. Курта П.А. Эффективная модель интерфейса взаимодействия пользователя с информационным сервисом запросного типа // Труды учебных заведений связи. 2023. Т. 9. № 6. С. 102-115. DOI: 10.31854/1813-324X-2023-9-6-102-115.
5. Курта П.А. Система статистического измерения атомарной эффективности графических элементов интерфейсов // Труды учебных заведений связи. 2024. Т. 10. № 6. С. 99-110. DOI: 10.31854/1813-324X-2024-10-6-99-110.

УДК 004.056

**СРАВНИТЕЛЬНЫЙ АНАЛИЗ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ РАЗНОЙ РАЗМЕРНОСТИ  
ДЛЯ ЗАДАЧИ ОБНАРУЖЕНИЯ ПОДОЗРИТЕЛЬНЫХ ПОЛЬЗОВАТЕЛЬСКИХ ЗАПРОСОВ****Лаврентьев Владимир Владимирович, Левшун Дмитрий Сергеевич**

СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия

e-mails: vvlavrentiev@yandex.ru, levshun.d@iiias.spb.su

**Аннотация.** В условиях стремительного развития больших языковых моделей (LLM) возрастает необходимость обеспечения их безопасности при взаимодействии с пользователями. Одной из ключевых задач в данной области является выявление и блокировка потенциально опасных запросов, включая обращение к табуированным темам и попытки эксплуатации уязвимостей типа Prompt Injection. Настоящее исследование посвящено определению оптимальной размерности LLM, предназначенной для дообучения на специализированных наборах данных с целью повышения её способности к детектированию и фильтрации вредоносных или небезопасных входных запросов. В работе проводится сравнительный анализ моделей различных масштабов (от малых до очень больших) по критериям качества выявления опасных запросов, устойчивости к атакам, затрат на обучение и инференс, а также способности к обобщению на ранее не встречавшиеся паттерны вредоносных промптов. Эксперименты включают дообучение моделей на синтетических и реальных наборах данных, содержащих как безопасные, так и вредоносные промпты, с последующим тестированием их на специально сконструированных сценариях атак. Результаты исследования позволяют установить компромисс между размерностью модели и её эффективностью в задачах обеспечения безопасности, а также выработать рекомендации по выбору архитектуры и стратегии дообучения LLM для использования в системах фильтрации и мониторинга пользовательских запросов. Работа вносит вклад в развитие методов безопасного применения генеративного искусственного интеллекта и может быть использована при разработке LLM-систем, устойчивых к манипуляциям и атакам через естественный язык.

**Ключевые слова:** информационная безопасность; большая языковая модель; защита от промпт инъекций; анализ производительности; фильтрация запросов.

**ARCHITECTURE OF A SYSTEM FOR PROTECTION OF SOLUTIONS BASED ON LARGE  
LANGUAGE MODELS FOR INTERNET OF THINGS DEVICES****Lavrentiev Vladimir, Levshun Dmitry**

St. Petersburg Federal Research Center of the Russian Academy of Sciences

39 14th Line VO, St. Petersburg, 199178, Russia

e-mails: vvlavrentiev@yandex.ru, levshun.d@iiias.spb.su

**Abstract.** With the rapid advancement of large language models (LLMs), there has been an increased need to ensure their security when interacting with users. One of the major challenges in this regard is identifying and preventing potentially harmful requests, such as access to sensitive topics or attempts to exploit vulnerabilities such as prompt injection. This study aims to determine the optimal size of large language models (LLMs) designed for advanced training on specialized datasets in order to improve their ability to detect and filter malicious or unsafe input. The paper compares models of various sizes, ranging from small to large, based on several criteria, including the quality of their detection of dangerous requests, their resistance to attacks, the costs associated with training and inference, and their ability to generalize to new patterns of malicious activity. Experiments involve further training the models on both synthetic and real datasets that contain safe and malicious software, followed by testing them in specially designed attack scenarios. Based on the results of this study, we can find a balance between the size of a model and its effectiveness in security tasks. Additionally, this study provides recommendations for choosing the appropriate architecture and training strategy when retraining LLMs for use in filtering and monitoring user requests. This work contributes to the advancement of techniques for the safe application of generative AI and can be utilized in the creation of LLM (large language model) systems that are resilient to manipulation and attack through natural language input.

**Keywords:** information security; large language model; protection against prompt injections; performance analysis; query filtering.

Целью данного исследования является определение оптимальной размерности большой языковой модели (LLM) для задач дообучения [1] и последующего использования в целях выявления потенциально опасных запросов, включая атаки типа промпт инъекций и обращения к табуированным темам.

На первом этапе проводится выбор языковых моделей различных масштабов с открытым исходным кодом, чтобы обеспечить воспроизводимость и гибкость в дообучении. Выбранные архитектуры включают:

- малые модели: ~125М–350М параметров (например, LLaMA 125M);
- средние модели: ~1.3B–7B параметров (например, LLaMA 2–7B, Falcon 7B);
- большие модели: ~13B+ параметров (например, LLaMA 2–13B, Falcon 13B).

Методология исследования включает несколько этапов. На первом этапе проводится предварительный отбор моделей различной размерности (от ~125 млн до ~13 млрд параметров), основанных на открытых архитектурах (например, GPT, LLaMA, Falcon), с последующим их дообучением на специализированных датасетах, содержащих метки «безопасный»/«небезопасный» запросС.

Для создания обучающего корпуса используются как реальные примеры вредоносных промптов (из открытых источников и специализированных репозиториях), так и синтетически сгенерированные атаки, включая попытки джейлбрейка, обходы фильтров, скрытые инструкции (obfuscated prompts) и контекстные инъекции [3].

Модели обучаются с использованием техник дообучения с учителем [4] для повышения способности различать тонкие семантические различия между безопасными и вредоносными запросами. Для оценки устойчивости моделей к атакам используется тестовый набор из ранее невиданных инъекций, включая обучение без примеров (zero-shot) и с малым количеством примеров (few-shot) сценарии.

Оценка эффективности моделей проводится с использованием следующих метрик:

- True Positive Rate и False Positive Rate — для оценки чувствительности и специфичности в обнаружении опасных запросов.
- Adversarial Success Rate — процент атак, приведших к обходу фильтрации.
- Latency и Resource Efficiency — для анализа производительности и затрат на инференс в зависимости от размерности модели.

Дополнительно проводится валидация реальным человеком, при которой эксперты по информационной безопасности вручную проверяют граничные случаи и ложные срабатывания, чтобы оценить пригодность моделей к реальному применению. Отметим, что процесс тестирования моделей в рамках исследования, направленного на выявление потенциально опасных запросов (включая промпт инъекции и рассуждения на табуированные темы), представляет собой многоэтапную и многоуровневую процедуру. Он включает как автоматизированные, так и экспертные методы оценки, направленные на проверку эффективности, устойчивости и адекватности моделей различной размерности.

Важно, что повторное тестирование [5] проводится на независимых выборках, а результаты логируются и агрегируются в виде отчетов и визуализаций (ROC-кривые, матрицы ошибок и др.). Пороговые значения подбираются с учетом компромисса между безопасностью и пользовательским опытом.

Результаты проведенного исследования демонстрируют, что выбор оптимальной размерности LLM существенно влияет на её способность эффективно и безопасно обрабатывать пользовательские запросы, включая выявление промпт инъекций и обращений к табуированным темам.

Работа вносит вклад в понимание взаимосвязи между масштабом модели, её обобщающей способностью и устойчивостью к вредоносным входам.

Было установлено, что модели среднего размера (2–7 млрд параметров) обеспечивают наилучший баланс между точностью классификации, устойчивостью к атакам и вычислительной эффективностью.

Контрастивное дообучение и использование разнообразных тестовых наборов позволяют существенно повысить чувствительность модели к скрытым и нетривиальным формам вредоносных запросов. Более того, LLM такой размерности могут быть безопасно встроены в решения для Интернета вещей [6].

С практической точки зрения, настоящее исследование предлагает воспроизводимую методологию оценки и дообучения LLM для задач фильтрации и мониторинга пользовательского ввода в LLM-системах. Это особенно важно для разработчиков безопасных ИИ-продуктов, чат-ботов, ассистентов и других систем, взаимодействующих с пользователями в открытом текстовом формате.

Предложенные метрики и подходы к тестированию могут быть использованы как основа для аудита и сертификации LLM по критериям безопасности.

Исследование подчёркивает необходимость интеграции механизмов активной фильтрации и оценки безопасности уже на этапе проектирования и масштабирования языковых моделей, что критически важно в условиях растущего числа угроз, связанных с генеративным ИИ.

#### СПИСОК ЛИТЕРАТУРЫ

1. Venkatesh Balavadhani Parthasarathy, Ahtsham Zafar, Aafaq Khan, Arsalan Shahid. The Ultimate Guide to Fine-Tuning LLMs from Basics to Breakthroughs: An Exhaustive Review of Technologies, Research, Best Practices, Applied Research Challenges and Opportunities // ArXiv [Электронный ресурс]. URL: <https://arxiv.org/pdf/2408.13296> (дата обращения: 21.08.2025).
2. Paul Karazuba. Unlocking The Power of Edge Computing with Large Language Models // Semiconductor Engineering [Электронный ресурс]. URL: <https://semiengineering.com/unlocking-the-power-of-edge-computing-with-large-language-models/> (дата обращения: 30.07.2024).
3. AIR Bench 2024. Набор данных для тестирования больших языковых моделей на уязвимости категории Prompt Injection <https://huggingface.co/datasets/stanford-crfm/air-bench-2024>.
4. Speed Always Wins: A Survey on Efficient Architectures for Large Language Models [Электронный ресурс]. URL: <https://arxiv.org/pdf/2508.09834> (дата обращения: 21.08.2025).
5. Лаврентьев В.В., Левшун Д.С. Архитектура системы для автоматизации выявления уязвимостей больших языковых моделей // XIII Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (АПИНО 2024). Санкт-Петербург, Россия, 27 - 28 февраля, 2024. Т. 1. С. 539-543.
6. Dmitry Levshun, Andrey Chechulin, Igor Kotenko, Yannick Chevalier. Design and verification methodology for secure and distributed cyber-physical systems. Proceedings of the 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS). IEEE, 2019. P. 1-5. DOI: 10.1109/NTMS.2019.8763814.

УДК 004.056

**ПРОБЛЕМАТИКА БЕЗОПАСНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ  
С ПОЗИЦИИ СИСТЕМНОГО АНАЛИЗА****Леонов Николай Викторович<sup>1</sup>, Буйневич Михаил Викторович<sup>2</sup>, Антонюк Евгений Артурович<sup>3</sup>**<sup>1</sup> Государственный научно-исследовательский институт прикладных проблем

Обводного канала наб., 29, Санкт-Петербург, 191167, Россия

<sup>2</sup> Санкт-Петербургский университет ГПС МЧС России

Московский пр., 149, Санкт-Петербург, 196105, Россия

<sup>3</sup> СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия

e-mails: leonov-nv@yandex.ru, bmv1958@yandex.ru, antonyuk@comsec.spb.ru

**Аннотация.** Рассматривается проблематика наличия уязвимостей в программном обеспечении с позиции системного анализа, для чего противодействие им сводится к оптимизационной задаче.

**Ключевые слова:** программное обеспечение; уязвимость; информационная безопасность; анализ.

**SOFTWARE SECURITY PROBLEMS FROM THE POSITION OF SYSTEM ANALYSIS****Leonov Nikolay<sup>1</sup>, Buinevich Mikhail<sup>2</sup>, Antonyuk Yevgeniy<sup>3</sup>**<sup>1</sup> Russian State Research Institute of Applied Problems

29 Obvodniy Kanal Emb, St. Petersburg, 191167, Russia

<sup>2</sup> St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia

149 Moskovskiy Av, St. Petersburg, 196105, Russia

<sup>3</sup> St. Petersburg Federal Research Center of the Russian Academy of Sciences

39 14th Line VO, St. Petersburg, 199178, Russia

e-mails: leonov-nv@yandex.ru, bmv1958@yandex.ru, antonyuk@comsec.spb.ru

**Abstract.** The problem of the vulnerabilities presence in software is considered from the standpoint of systems analysis, for which counteraction to them is reduced to an optimization task.

**Keywords:** software; vulnerability; information security; analysis.

Небезопасность используемого программного обеспечения (ПО) является актуальной проблематикой большинства сфер современного мира. Способы же противодействия основному фактору этого [1] — уязвимостям программ — носят частный характер, что не позволяет получить качественного прорыва в разрешении данной проблемы. Так, хотя давно существует и активно развивается антивирусное ПО, его функционал как правило оказывается запаздывающим (например, сигнатуры новых уязвимостей) по отношению к создаваемым злоумышленниками угрозам. Запрет на уровне законодательства на использование средств анализа программного кода (например, дизассемблеров, декомпиляторов и пр.) хотя и затруднит злоумышленнику создание эксплойтов, однако аналогичным образом снизит эффективность работы экспертов по безопасности программного кода, выполняющих подобные операции. Не системное же регулирование всей ИТ-сферы не столько помешает разработке вредоносного ПО, сколько усложнит работу рядовых программистов.

Указанные примеры очередной раз подчеркивают необходимость системного подхода к проблеме, позволяя свести задачу по ее разрешению к оптимизационной — когда требуется управление стратегическими параметрами области ПО, влияющими сложным и, частично, стохастическим образом [2] на информационную безопасность (ИБ). Так, в качестве параметров может использоваться степень контроля за использованием определенных сущностей предметной области — методов, программно-аппаратных средств, человеческого ресурса и т.п., а в качестве целевой функции — кортеж из частных и оптимизируемых, таких, как прогнозируемое количество уязвимостей на будущем периоде, уровень подготовки разработчиков ПО, востребованность в узкоспециализированных экспертах по ИБ; скорее всего, частные функции будут конфликтовать между собой, что потребует поиска приемлемых (т.е. рациональных) решений. Также, согласно классической постановке задачи системного анализа, у параметров существуют ограничения, например, невозможность полного отказа от использования ряда методов или средств области ПО. Нужно отметить, что помимо «подбора» параметров для целевой функции одним из подходов к разрешению проблемы может быть создание новых сущностей области и их связей.

Применение системного подхода в части решения оптимизационной задачи может быть осуществлено следующим образом. Требуется создание модели предметной области — противодействие уязвимостям ПО, отражающей в аналитическом виде все сущности и их связи. Модель должна учитывать вероятностные факторы, что является следствием сложности объектов реального мира и девиативного поведения его субъектов [3]. Для решения оптимизационной задачи могут быть применены как классические и интеллектуальные методы. И, наконец, система должна обладать функционалом для поддержки принятия решений ИБ-руководителем.

**СПИСОК ЛИТЕРАТУРЫ**

1. Леонов Н.В. Противодействие уязвимостям программного обеспечения. Часть 1. Онтологическая модель // Вопросы кибербезопасности. 2024. № 2 (60). С. 87-92. DOI: 10.21681/2311-3456-2024-2-87-92.
2. Батов В.Ю., Драчев В.О., Мамаев Е.В. К вопросу выбора политики безопасности на основе решения оптимизационных задач // Научные проблемы материально-технического обеспечения Вооружённых Сил Российской Федерации. 2019. № 2 (12). С. 25-37.
3. Буйневич М.В., Моисеенко Г.Ю. Повышение «устойчивости» регламентов деятельности как способ противодействия неумышленному инсайдингу // Вопросы кибербезопасности. 2024. № 6 (64). С. 108-116. DOI: 10.21681/2311-3456-2024-6-108-116.

УДК 004.4:004.056

**ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: РОЛЬ ТРЕБОВАНИЙ  
И АРХИТЕКТУРЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ****Литвинов Евгений Николаевич, Ананьева Варвара Яновна**

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

Профессора Попова ул., 5, Санкт-Петербург, 197022, Россия

e-mail: lit\_evgeniy@mail.ru, viaananeva@etu.ru

**Аннотация.** В материалах рассматриваются ключевые аспекты информационной безопасности на всех этапах разработки информационной системы. Особое внимание уделяется распространённым ошибкам при сборе и анализе требований и проектировании системы, которые приводят к уязвимостям. Предложены практические решения, включая использование международных стандартов безопасности и современных инструментов защиты. Материал содержит конкретные примеры уязвимостей и рекомендации по их предотвращению. Статья будет полезна аналитикам, разработчикам, архитекторам и специалистам по информационной безопасности.

**Ключевые слова:** информационная безопасность; жизненный цикл разработки ПО; анализ требований; проектирование архитектуры; стандарты безопасности; уязвимости в информационной системе.

**INFORMATION SECURITY: THE ROLE OF REQUIREMENTS AND ARCHITECTURE  
OF THE INFORMATION SYSTEM****Litvinov Evgeniy, Ananeva Varvara**

Saint-Petersburg Electrotechnical University

5 Professor Popov St, St. Petersburg, 197022, Russia

e-mail: lit\_evgeniy@mail.ru, viaananeva@etu.ru

**Abstract.** The article discusses the key aspects of information security at all stages of software development. Special attention is paid to common errors in requirements gathering and analysis and system design that lead to vulnerabilities. Practical solutions, including the use of international security standards and modern protection tools, are offered. The material contains specific examples of vulnerabilities and recommendations for their prevention. This article will be useful for analytics, developers, architects and information security specialists.

**Keywords:** information security; software development lifecycle; requirements analysis; architecture design; security standards; information system vulnerabilities.

Проблема безопасности информационных систем является одной из важнейших при их разработке [1]. Никому из пользователей не хотелось бы попасть в ситуацию, когда система имеет доступ к личным данным, и при этом имеет уязвимости, которые смогут использовать злоумышленники, например, в целях похищения денежных средств [2]. Поэтому компании, разрабатывающие программное обеспечение (ПО), обращают большое внимание на информационную безопасность [3].

*Этапы разработки и их влияние на безопасность готовой системы.* Существуют различные методологии разработки ПО [4]. Каждая команда выбирает свою методологию для достижения определенных целей и решения задач. Популярные методологии, которые могут быть положены в основу своей методологии (которую можно рассматривать как смешение нескольких) — это каскадная, V-образная, инкрементная [4]. Также команды разработчиков используют принципы Agile, которые фокусируются на гибкости и тесном взаимодействии команды разработки и заказчика [4]. Рассмотрим создание ПО на примере каскадной методологии. Разработка состоит из следующих основных этапов: сбор и анализ требований, проектирование, реализация, верификация, поддержка и эксплуатация системы, вывод из эксплуатации [5]. На каждом шаге необходимо предпринимать меры по обеспечению безопасности системы [3]. Разберём каждый из этапов. На этапе сбора и анализа требований выявляются и фиксируются характеристики, поведение системы для дальнейшей её разработки, также при этом особое внимание уделяется аспектам информационной защиты. На данном этапе важно учесть все сценарии, в том числе закрыть «дыры» безопасности. На следующем шаге, проектировании архитектуры, предпринимаются основные меры по безопасности системы, так как на данном этапе закладывается фундамент (выбор архитектуры, интеграции, базы данных) будущей системы. При реализации важно, чтобы разработчики выполнили работу в соответствии с поставленными требованиями. Один из главных этапов для безопасности системы — это верификация (тестирование). Здесь необходимо проверить все возможные сценарии, которые могут привести к утечке данных и другим видам уязвимостей. Следующий этап - эксплуатация и поддержка. При запуске системы пользователи нередко находят баги и, что особенно важно, «дыры» в системе безопасности. На этапе поддержки должны быть произведены мероприятия по выявлению (с помощью пользователей) и устранения таких уязвимостей. При выводе из эксплуатации важно также обеспечить безопасность хранящихся ранее в системе данных, удалить их и связанную с ними информацию, также, в частности, используя различные стандарты. Таким образом, на каждом этапе разработки системы важно предпринимать меры для безопасного использования системы.

*Ошибки, допускаемые на начальных стадиях разработки, с точки зрения безопасности системы.* Рассмотрим самые распространённые ошибки при анализе требований и проектировании. Аналитики часто концентрируются на функциональных требованиях, уделяя меньше времени нефункциональным, что в том числе

приводит к пропускам сценариев, которые приводят к незащищённости системы. Как пример можно привести требование: «Пользователь должен иметь возможность авторизоваться», — но в данном случае нет описания уровня защиты. Также тяжело предсказать все возможные уязвимости, например, тяжело предусмотреть взлом изнутри. Встречаются проблемы с копированием требований из других проектов без адаптации под разрабатываемую систему, как вариант, требование «Шифровать все данные с помощью хеширования» без учёта, какие именно данные критичны.

Что касается этапа проектирования, здесь возможны несколько проблем, разберём их. Во-первых, в случае микросервисной архитектуры не должно создаваться ситуации, когда взлом одного компонента приводит к компрометации остальных. При этом микросервисы подразумевают масштабируемость, что также должно отражаться на защите системы. Во-вторых, при проектировании системы происходит выбор технологий, с помощью которых будет создаваться система. Так как злоумышленники все время ищут уязвимости, не стоит использовать устаревшие и небезопасные технологии. Также отдельно стоит отметить методы шифрования, которыми нельзя пренебрегать. Если выбрать алгоритм с недостаточной стойкостью, разработанную систему будет легче взломать. В-третьих, возможны ситуации, когда защита пройдена злоумышленником. В таком случае необходимо предусматривать многоуровневую защиту. Данный метод актуален для особо важных компонентов системы, чтобы уменьшить вероятность взлома. В-четвертых, злоумышленники могут воспользоваться «слепыми пятнами» безопасности. Данные случаи допускаются при узком взгляде аналитика на возможные варианты взлома системы. В качестве примера можно привести ситуацию, когда разработчики защитили веб-приложение от SQL-инъекций, но забыли про риск подделки SMS-сообщений для 2FA (атака SIM-swapping).

Эти проблемы нельзя полностью искоренить, но необходимо минимизировать. Далее рассмотрим, какие для этого есть решения.

Обеспечение безопасности на начальных этапах разработки системы. Для проектирования безопасной системы существуют международные (ISO 27001 [1], OWASP ASVS, PCI DSS [2]) и национальные (ГОСТ Р ИСО/МЭК 27001-2021 [1]) стандарты безопасности. Аналитику необходимо придерживаться данных стандартов во время сбора и анализа требований, а также проектирования. Кроме этого, для обеспечения безопасности, помогают диаграммы (DFD, BPMN, UML). При построении диаграмм проще отследить неучтенные в результате сбора и анализа требований сценарии. Также надо учитывать, что микросервисная архитектура безопаснее монолитной. Защиту улучшает возможность изоляции компонентов друг от друга, что невозможно в случае монолита. Говоря о шифровании, важно отметить необходимость использования актуальных стандартов, которые не приведут к взлому системы. Также для лучшей защиты системы можно использовать технологии безопасного хранения паролей, API-ключей, сертификатов. Хорошо подойдут HashiCorp Vault (шифрует секреты, выдает их по запросу с проверкой прав), AWS Secrets Manager (интеграция с AWS-сервисами, автоматическая ротация паролей).

В ходе работы были рассмотрены этапы разработки и выявлены ключевые ошибки, допускаемые на начальных стадиях разработки. Нельзя не сказать о важности роли аналитика. Ему необходимо рассмотреть все сценарии, чтобы не допустить уязвимости. По результатам исследования можно сказать об особой важности этапов сбора и анализа требований, а также проектирования для обеспечения безопасности разрабатываемой системы.

#### СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р ИСО/МЭК 27001-2021 «Информационная безопасность, кибербезопасность и защита приватности. Системы менеджмента информационной безопасности. Требования». М.: Стандартинформ, 2021. 36 с.
2. Payment Card Industry (PCI) Data Security Standard, Version 4.0 [Электронный ресурс]. Режим доступа: <https://www.pcisecuritystandards.org/> (дата обращения: 25.06.2025).
3. ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения». М.: Стандартинформ, 2016. 24 с.
4. Фаулер М. Архитектура корпоративных программных приложений: пер. с англ. М.: Вильямс, 2019. 544 с.
5. NIST Special Publication 800-64 Revision 2 «Security Considerations in the System Development Life Cycle» [Электронный ресурс]. Режим доступа: <https://csrc.nist.gov/publications/detail/sp/800-64/rev-2/final> (дата обращения: 25.06.2025).

УДК 004.056.5

#### КОМПЛЕКСНЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ МОБИЛЬНЫХ УСТРОЙСТВ: УГРОЗЫ, УЯЗВИМОСТИ, ЗАЩИТА

Лукашенко Василий Ильич, Яровой Роберт Владимирович

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: lukasenkvasilij@gmail.com, Nadzar@yandex.ru

**Аннотация.** Мобильные устройства всё чаще становятся целями кибератак, сочетающих технические уязвимости с социальной инженерией. В тезисе изложены ключевые угрозы, от малвари до MITM-атак, и способы противодействия — от шифрования до поведения пользователя. Подчеркивается необходимость сочетания технических, организационных и поведенческих мер в обеспечении безопасности повседневного цифрового пространства.

**Ключевые слова:** мобильная безопасность; вредоносное ПО; фишинг; Wi-Fi-атаки; MITM, антивирус; шифрование; конфиденциальность; мобильные угрозы.

## COMPREHENSIVE ASPECTS OF MOBILE DEVICE SECURITY: THREATS, VULNERABILITIES, PROTECTION

Lukashenok Vasily, Yarovoy Robert

Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: lukashenokvasilij@gmail.com, Nadzar@yandex.ru

**Abstract.** Mobile devices are increasingly becoming targets for cyberattacks that combine technical vulnerabilities with social engineering. The paper outlines key threats, from malware to MITM attacks, and countermeasures, from encryption to user behavior. It emphasizes the need to combine technical, organizational, and behavioral measures to ensure the security of everyday digital space.

**Keywords:** mobile security; malware; phishing; Wi-Fi attacks; MITM; antivirus; encryption; privacy; mobile threats.

Рост использования смартфонов и планшетов обусловил расширение поверхности киберугроз, сопряжённых с высокой плотностью хранения личной и коммерчески значимой информации. Современные мобильные платформы уязвимы к целому спектру воздействий: от вредоносного ПО и фишинга — до атак через публичные сети и сторонние приложения [1, 2].

Наиболее распространёнными угрозами выступают трояны, шпионские модули, руткиты и рекламное ПО, часто встраиваемые в легитимные приложения. Примеры вроде «Triada» или «Pegasus» демонстрируют, что предустановленное ПО и эксплойты в системных службах создают возможность слежки и управления устройством без ведома владельца. Дополнительный вектор опасности формируется фишингом и социальной инженерией — с помощью СМС, писем и поддельных сайтов [3, 4].

Особую опасность представляют атаки в публичных Wi-Fi-сетях, реализуемые по сценарию «человек посередине». Подмена точек доступа, перехват незашифрованного трафика и внедрение вредоносного содержимого делают такие подключения критически уязвимыми. Использование VPN, проверка сертификатов и ограничение доступа к чувствительным данным — базовые контрмеры, однако они не всегда реализуются в пользовательском поведении.

Для обеспечения мобильной безопасности необходима комплексная защита: регулярное обновление ОС, использование антивирусов, шифрование, настройка прав приложений, а также внедрение двухфакторной аутентификации. Механизмы защиты, встроенные в системы Android и iOS, усиливаются за счёт стороннего ПО, но основную роль продолжает играть поведенческая осмотрительность пользователя.

Безопасность мобильных устройств — это не просто технологический вопрос, а совокупность грамотной архитектуры, правильных привычек и минимизации цифрового следа. Обнаружение угроз в реальном времени, отказ от использования неофициальных приложений, внимательное отношение к правам доступа и контроль сетевого окружения становятся условиями сохранения цифровой автономии в условиях экспоненциального роста атакующих техник.

### СПИСОК ЛИТЕРАТУРЫ

1. Гладких А.А., Дементьев В.Е., Чилихин Н.Ю. Основы современных криптографических систем и перспективы их развития: учебное пособие. Ульяновск: УлГТУ, 2020. 214 с.
2. Яровой Р.В., Рябов Г.А., Карганов В.В. Кибербезопасность в мире инфотелекоммуникаций: вызовы и стратегии защиты // инновационная деятельность в Вооруженных Силах Российской Федерации. 2023. С. 373-377
3. Яровой Р.В., Рябов Г.А., Изотов Д.Ю. Вредоносное программное обеспечение: типы, методы распространения и антивирусные меры // Тенденции развития науки и образования. 2023. № 101-4. С. 99-101
4. Лысенко А. В., Анализ методов обнаружения вредоносных программ // Молодой ученый. 2016. № 21 (125). С. 758-761.

УДК 004.056

## СОЗДАНИЕ НАБОРА ДАННЫХ ДЛЯ ЗАДАЧ БЕЗОПАСНОСТИ ВОДООЧИСТНЫХ СООРУЖЕНИЙ

Мелешко Алексей Викторович

СПб ФИЦ РАН

14 линия ВО, 39, Санкт-Петербург, 199178, Россия

e-mail: meleshko.a@iiias.spb.su

**Аннотация.** Для разработки интеллектуальных средств обнаружения атак в киберфизических системах необходимо наличие больших обучающих наборов данных, учитывающих как различные режимы функционирования системы, так и разнообразные деструктивные воздействия на нее. В работе описываются основные проблемы получения исходных данных для создания и настройки средств обнаружения атак и вторжений. Представлен подход к созданию набора данных киберфизической системы водоочистки с учетом возможных деструктивных воздействий на нее, который позволит создавать наборы данных большого объема, пригодные для использования при обучении средств обнаружения атак, за приемлемое время. Генерируемые данные моделируют функционирование системы водоочистки, основанной на процессе отстаивания взвешенных частиц в воде. В основе метода генерации данных лежит общепринятый математический аппарат процесса отстаивания воды, в частности используются законы Торричелли и Стокса для программного моделирования

процессов течения жидкости и оседания взвешенных частиц. В работе также сформулированы атаки, релевантные для систем водоочистки данного типа. Обсуждаются способы валидации достоверности и корректности разработанного метода с учетом реальных данных, получаемых от натурного прототипа горизонтального отстойника.

**Ключевые слова:** киберфизические системы; безопасность киберфизических систем; генерация наборов данных; безопасность водоочистных сооружений; кибератаки.

## CREATION OF A DATA SET FOR WATER TREATMENT SECURITY TASKS

Meleshko Aleksei

St. Petersburg Federal Research Center of the Russian Academy of Sciences

39 14th Line VO, St. Petersburg, 199178, Russia

e-mail: meleshko.a@iiias.spb.su

**Abstract.** To develop intelligent attack detection tools in cyber-physical systems, it is necessary to have large training datasets that take into account both the various modes of operation of the system and the various destructive effects on it. The paper describes the main problems of obtaining source data for creating and configuring attack and intrusion detection tools. An approach is presented to create a dataset of a cyberphysical water treatment system, taking into account possible destructive effects on it, which will allow creating large-volume datasets suitable for use in training attack detection tools in an acceptable time. The generated data models the functioning of a water treatment system based on the process of settling suspended particles in water. The data generation method is based on the generally accepted mathematical apparatus of the water settling process, in particular, the Torricelli and Stokes laws are used for software modeling of fluid flow and sedimentation of suspended particles. The paper also formulates attacks that are relevant for this type of water treatment systems. The methods of validating the reliability and correctness of the developed method are discussed, taking into account real data obtained from a full-scale prototype of a horizontal sump.

**Keywords:** cyber-physical systems; cyber-physical systems security; dataset generation; water treatment system security; cyber attacks.

Киберфизические системы (КФС) в настоящее время используются в множестве различных сфер деятельности. Производственная промышленность, очистка сточных вод, транспортная промышленность — это лишь малый список сфер применения КФС. Такие системы интегрируются в физические процессы среды и позволяют контролировать любые ее изменения и работать автономно с минимальным участием человека. Однако, внедрение КФС в критически важные отрасли требует обеспечения их безопасности и защиты от различных информационных атак. Важную роль при разработке механизмов защиты КФС на основе методов искусственного интеллекта играют исходные данные. Наличие качественных и достоверных наборов данных позволяет проектировать модели обнаружения атак и аномалий, а также тестировать эффективность систем обнаружения вторжений. Однако, в большинстве случаев получение доступа к реальным наборам данных затруднено в силу требований регулирующих документов в сфере обеспечения информационной безопасности критических объектов.

Настоящая работа посвящена разработке подхода к генерации наборов данных КФС очистки воды на примере процесса отстаивания вода (седиментации). Атаки на системы водоочистки могут приводить к значительному материальному и экологическому ущербу, включая природные катастрофы. Общедоступные наборы данных в области водоочистки имеют ряд недостатков, таких как отсутствие специфичных для предметной области данных и атак. Новизна данной работы заключается в определении комплексного подхода к созданию наборов данных для задач безопасности систем водоочистки, который позволит получить наборы данных, пригодные для обучения и настройки механизмов обнаружения атак.

Для формирования основных принципов и требований к программному комплексу генерации данных был выполнен анализ релевантных работ. В [1] авторы описывают методологию генерации наборов данных для безопасности промышленных систем водоочистки. Выделены основные требования к генерируемым наборам данных, такие как наличие в наборе данных как показания от сенсоров и исполнительных устройств, так и сетевые данные, и данные различных системных журналов. Кроме того, набор данных должен содержать в себе атаки и аномалии, и их разметку. Предложенная авторами методология состоит из нескольких шагов, но он является обобщенным и не связан с какой-либо конкретной системой водоочистки. Авторы [2] проводят моделирование кибератак на объекты ядерной промышленности и генерацию набора данных используя виртуальные КФС. Авторами была разработана виртуальная КФС для моделирования кибератак и генерации наборов данных кибератак. Таким образом было сгенерировано два набора данных — набор данных с показаниями физических датчиков и набор данных с логами самой КФС. Разметку набора данных авторы реализовали с помощью метки времени, что позволило более эффективно обнаруживать аномалии. В [3] авторы проводят математическое моделирование процессов бытовой очистки воды, которые протекают в анаэробных септиках. Авторы предложили три математические модели кинетики первого для моделирования системы очистки сточных вод. А именно модель для септика, анаэробного фильтра и полей фильтрации. Для проверки корректности математической модели авторы использовали набор данных, полученный на станции очистки сточных вод, которая была построена для очистки массивных загрязненных бытовых сточных вод. Таким образом, можно сделать выводы, что на текущий момент отсутствует единый подход к формированию наборов



данных, которые бы учитывал не только функционирования системы, но и вредоносные воздействия на нее, а также имеется ряд практических пробелов. В частности, некоторые работы описывают только методологию для создания наборов данных, но не проводят алгоритмы их генерацию. Часть работ обсуждает теоретические аспекты моделирования, но не предоставляет инструменты для генерации данных или готовых наборов данных.

Подход, который предложен в данной работе направлен на генерацию набора данных для процесса отстаивания воды, то есть седиментации. Для валидации набора используется программно-аппаратный прототип такого очистного сооружения, а именно горизонтальный отстойник. Прототип содержит в себе три резервуара, датчики уровня воды и мутности воды, и исполнительные механизмы (управляемые краны) для движения жидкости между резервуарами. Очистка воды реализуется посредством отстаивания взвешенных частиц на дно резервуара отстойника и последующим сбросом очищенной воды в другой резервуар.

Предлагаемый в данной работе подход состоит из нескольких этапов: (1) описание технологического процесса водоочистки, (2) математическое моделирование процессов водоочистки, (3) генерация набора данных нормального функционирования системы, выявление актуальных видов атак, (4) внедрение атак в набор данных, (5) валидация набора данных. На первом этапе проводится описание технологического процесса очистки воды, а именно процесса осаждения взвешенных частиц. На этапе математического моделирования проводится разработка математического аппарата осаждения взвешенных частиц и движения жидкости между резервуарами. В качестве математической модели движения жидкости используется закон Торричелли, а для осаждения взвешенных частиц - закон Стокса. На основе данных законов вычисляется динамика изменения показаний сенсоров в резервуарах. На третьем этапе проводится моделирование работы системы водоочистки без воздействия каких-либо атак, включая этап выхода системы на нормальный режим функционирования. Этап реализации и внедрения атак включает в себя определение модели атак. В данном случае она формулируется как манипуляция/подмена данных сенсоров и исполнительных механизмов. Были определены модели атаки переполнения резервуара отстойника, атаки добавления большого объема несанкционированной загрязненной воды в резервуар отстойник, атаки превышения допустимого потока загрязненной воды через резервуар отстойник, атаки на исполнительные механизмы, атака подмены показаний датчиков системы. Последний этап валидации необходим для оценки точности полученного набора данных и проводится путем сопоставления полученных данных с данными от реального прототипа.

Таким образом, в данной работе был описан подход к генерации набора данных для водоочистного сооружения, а именно для горизонтального отстойника. Были выделены основные виды атак на подобные системы, разработана математическая модель физических процессов, протекающих в процессе отстаивания загрязненных вод. Дальнейшее направление работ связано с валидацией сгенерированных данных относительно реальных, полученных с натурального прототипа аналогичной системы.

*Исследование выполнено за счет гранта Российского научного фонда № 23-11-20024.*

#### СПИСОК ЛИТЕРАТУРЫ

1. Novikova E., Doynikova E., Saenko I. Methodology for Dataset Generation for Research in Security of Industrial Water Treatment Facilities // International Russian Automation Conference (RusAutoCon). 2023. pp. 953-958. doi: 10.1109/RusAutoCon58002.2023.10272930.
2. Xiao Y., Dong F., Chen S., & Demachi K. Datasets Generation with Virtual Cyber Physical System Design and Cyber-Attack Simulation on Nuclear Facilities // Proceedings of the INMM 64th Annual Meeting. 2023. pp. 1-6.
3. Fernández del Castillo, A.; Verduzco Garibay, M.; Senés-Guerrero, C.; Yebra-Montes, C.; de Anda, J.; Gradilla-Hernández, M.S. Mathematical Modeling of a Domestic Wastewater Treatment System Combining a Septic Tank, an Up Flow Anaerobic Filter, and a Constructed Wetland // Water. 2020. vol. 12. № 3019. doi: 10.3390/w12113019.

УДК 004.056

#### ОБНАРУЖЕНИЕ АНОМАЛИЙ В КОНТЕЙНЕРНЫХ СИСТЕМАХ НА ОСНОВЕ ПРОФИЛИРОВАНИЯ ПАРАМЕТРОВ БЕЗОПАСНОСТИ

**Мельник Максим Владимирович, Котенко Игорь Витальевич**  
СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия  
e-mails: mkmxvh@gmail.com, ivkote@comsec.spb.ru

**Аннотация.** Архитектурные и эксплуатационные особенности контейнерных систем ставят под угрозу не только контейнеры, расположенные в операционной системе, но и саму операционную систему в целом. В работе представлена методика обнаружения аномального поведения контейнерных систем на основе профилирования и анализа параметров безопасности используемых при эксплуатации таких систем.

**Ключевые слова:** информационная безопасность; обнаружение аномалий; машинное обучение; контейнеры; профилирование параметров безопасности.

#### ANOMALIES DETECTION IN CONTAINER SYSTEMS BASED ON SECURITY PARAMETER PROFILING

**Melnik Maxim, Kotenko Igor**

St. Petersburg Federal Research Center of the Russian Academy of Sciences  
39 14th Line VO, St. Petersburg, 199178, Russia  
e-mails: mkmxvh@gmail.com, ivkote@comsec.spb.ru

**Abstract.** Architectural and operational features of container systems pose a threat not only to containers located in the operating system, but also to the operating system as a whole. The paper presents a method for detecting anomalous behavior of container systems based on profiling and analysis of security parameters used in the operation of such systems.

**Keywords:** information security; anomaly detection; machine learning; containers; profiling of security parameters.

В настоящее время контейнерные системы, как и любые среды выполнения программного кода подвержены множеству проблем безопасности. Такие проблемы возникают не только из-за существующих уязвимостей и недостатков безопасности, но и архитектурных и эксплуатационных особенностей таких систем [1]. Кроме того, применение злоумышленниками методов искусственного интеллекта для совершенствования тактик и техник эксплуатации несет дополнительные риски. В результате чего стабильная и качественная работа таких систем может быть нарушена в результате деструктивного воздействия. Таким образом, одной из главных задач обеспечения безопасности контейнерных систем является обнаружение аномалий в поведении контейнерных систем. В [2] используется подход, при котором анализируется поведение контейнерной системы на основе системных вызовов. В [3], напротив, анализируются показатели производительности контейнера. Однако, представленные подходы не всегда могут быть эффективными, особенно если природа аномалии никак не связана с вычислительными ресурсами или ее обнаружение невозможно посредством системных вызовов. Как в случае атаки Container Escape [4], во время которой выполняется монтирование диска хостовой операционной системы из контейнера.

В данной работе представлен подход к обнаружению аномального поведения контейнерных систем, основанный на профилировании параметров безопасности на базе машинного обучения. Предложено множество подходов к обнаружению аномалий на основе машинного обучения [1, 5, 6]. Для обучения моделей нейронной сети используется профиль, представляющий собой последовательность параметров (точки монтирования, сетевые интерфейсы, Capabilities, списки разрешенных системных вызовов и другие) на заданном интервале времени с единичным смещением. Для экспериментального подтверждения эффективности предлагаемого подхода разработан испытательный стенд, который состоит из виртуальной машины Ubuntu 22.04, двух контейнеров (ssh-сервер и контроллер домена) и программного компонента сбора данных. Оценка эффективности предложенного подхода выполнялась на обученных моделях нейронной сети с использованием показателей Accuracy, Precision, Recall и F1-score. Каждая модель была обучена в соответствии с профилем параметров безопасности. В заключении стоит отметить, что предложенный подход может быть использован как дополнительное средство обнаружения аномального поведения на основе анализа показателей производительности и системных вызовов.

*Исследование выполнено за счет гранта Санкт-Петербургского научного фонда № 23-РБ-01-09.*

#### СПИСОК ЛИТЕРАТУРЫ

1. Котенко И. В., Мельник М. В. Обнаружение атак и аномалий в контейнерных системах: подходы на основе сигнатур и правил // Искусственный интеллект и принятие решений. 2025. № 1. С. 3-13.
2. Snehi J., Bhandari A., Baggan V., Snehi M., Kaur H. AIDAAS: Incident handling and remediation anomaly-based IDaaS for cloud service providers // 2021 10th International Conference on System Modeling & Advancement in Research Trends (SMART). IEEE. 2021. P. 356-360.
3. Gupta S., Muthiyar N., Kumar S., Nigam A., Dinesh D. A. A supervised deep learning framework for proactive anomaly detection in cloud workloads // 14th IEEE India Council International Conference (INDICON). IEEE. 2017. P. 1-6.
4. Jarkas O., Ko R., Dong N., Mahmud R. A Container Security Survey: Exploits, Attacks, and Defenses // ACM Computing Surveys. 2025. Vol. 57. № 7. P. 1-36.
5. Branitskiy A., Kotenko I. Hybridization of computational intelligence methods for attack detection in computer networks // Journal of Computational Science. 2017. Vol.23. P.145-156.
6. Laskov P., Schäfer C., Kotenko I. Intrusion Detection in Unlabeled Data with Quarter-Sphere Support Vector Machines // Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft für Informatik (GI). 2004. P.71-82.

УДК 003.26

#### СПОСОБЫ УСИЛЕНИЯ РАНДОМИЗАЦИИ В АЛГЕБРАИЧЕСКИХ АЛГОРИТМАХ ЦИФРОВОЙ ПОДПИСИ СО СКРЫТОЙ ГРУППОЙ

Морозова Елена Владимировна<sup>1</sup>, Костина Анна Александровна<sup>2</sup>

<sup>1</sup> Государственный университет морского и речного флота имени адмирала С.О. Макарова  
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия

<sup>2</sup> СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия  
e-mails: lenmor@mail.ru, to.ann@inbox.ru

**Аннотация.** Алгоритмы цифровой подписи на конечных некоммутативных алгебрах, основанные на вычислительной трудности решения больших систем степенных уравнений, перспективны как постквантовые рандомизированные криптосхемы. Их особенностью является использование подгоночного элемента подписи в виде вектора (элемента алгебры), используемой в качестве носителя алгоритма. При фиксированном секретном ключе этот элемент принимает значения из ограниченного подмножества элементов алгебры. Последнее обуславливает невозможность обеспечения безусловной стойкости к атакам на основе произвольного числа известных подписей. Стойкость к данному типу атак в алгебраических алгоритмах подписи имеет

вычислительную природу, и их разработка ведется с учетом применения таких способов рандомизации подписи, при которых уровень вычислительной стойкости является достаточно высоким, не ниже стойкости к прямой атаке. Рассматриваются способы усиления рандомизации подписи, состоящие в повышении мощности множества значений, принимаемых подгоночным элементом подписи при фиксированном секретном ключе.

**Ключевые слова:** компьютерная безопасность; криптография; цифровая подпись; некоммутативные алгебры; ассоциативные алгебры; рандомизация подписи.

## METHODS FOR ENHANCED RANDOMIZATION IN ALGEBRAIC HIDDEN GROUP DIGITAL SIGNATURE ALGORITHMS

Morozova Elena<sup>1</sup>, Kostina Anna<sup>2</sup>

<sup>1</sup> Admiral Makarov State University of Maritime and Inland Shipping  
5/7 Dvinskaya St., St. Petersburg, 198035, Russia

<sup>2</sup> St. Petersburg Federal Research Center of the Russian Academy of Sciences  
39, 14-th Linia, VI, St. Petersburg, 199178, Russia  
e-mails: lenmor@mail.ru, to.ann@inbox.ru

**Abstract.** Digital signature algorithms on finite non-commutative algebras, based on the computational difficulty of solving large systems of power equations, are promising as post-quantum randomized cryptoschemes. Their feature is the use of a fitting signature element in the form of a vector (an algebra element) used as a carrier of the algorithm. With a fixed secret key, this element takes values from a limited subset of algebra elements. The latter determines the impossibility of providing unconditional resistance to attacks based on an arbitrary number of known signatures. Security to this type of attack in algebraic signature algorithms has a computational nature and their development is carried out taking into account the use of such signature randomization methods, in which the level of computational s is sufficiently high, not lower than resistance to a direct attack. Methods for enhancing signature randomization are considered, consisting in increasing the power of the set of values that are taking on by the fitting signature element, when the secret key is fixed.

**Keywords:** computer security; cryptography; digital signature; non-commutative algebras; associative algebras; signature randomization.

В текущий момент времени разработка практических постквантовых схем электронной цифровой подписи (ЭЦП) остается актуальной проблемой. Для решения последней перспективным является направление разработки рандомизированных алгоритмов ЭЦП на  $m$ -мерных ( $m = 4, 6, \dots, 25$ ) конечных некоммутативных ассоциативных алгебрах (КНАА), стойкость которых базируется на вычислительной трудности решения больших систем степенных уравнений (БССУ) [1, 2]. Для решения последней вычислительной задачи квантовый компьютер не является эффективным, что лежит в основе постквантовой стойкости (стойкости к атакам с использованием квантового компьютера) указанных алгебраических алгоритмов. Как и положено в рандомизированных схемах ЭЦП генерируемая подпись включает два параметра — рандомизирующий элемента подписи в виде натурального многозначного числа  $e$  и подгоночный элемент в виде  $m$ -мерного вектора  $S$ . Характерной особенностью последних является использование скрытой коммутативной группы и случайного выбора векторов  $G$  из этой группы для вычисления подгоночного элемента подписи  $S$  в зависимости от некоторых фиксированных секретных векторов  $D$  и  $F$  (элементов секретного ключа), например, по формуле  $S = DGF$ . При построении рассматриваемых схем ЭЦП в качестве алгебраического носителя используются КНАА, в которых легко задать скрытую группу достаточно большого порядка, при котором для каждого подписываемого электронного документа формируется уникальное значение подгоночного элемента  $S$ , принимающего значения вне скрытой группы. Однако, как показано в [3], число потенциально возможных значений  $S$  равно порядку скрытой группы и составляет малую долю от порядка используемой КНАА. Это создает предпосылки недостаточности рандомизации ЭЦП в том смысле, что атака на основе некоторого набора известных подписей имеет недостаточную вычислительную сложность для потенциального нарушителя. В связи с этим возникает необходимость усиления рандомизации подписи, т.е. применения механизмов рандомизации подписи, при которых существенно возрастает число различных значений, принимаемых элементом  $S$  по сравнению с приведенной выше формулой.

В работе [4] предложен критерий достаточности (достаточной полноты) рандомизации, как обеспечения стойкости к атакам на основе известных подписей, равной или превышающей стойкость к прямой атаке, заключающейся в решении БССУ в конечном поле, которая записывается по векторным уравнениям, связывающим элементы секретного и открытого ключей. Данный критерий можно дополнить случаем обеспечения 256-битного уровня стойкости к атакам на основе известных подписей, что устраняет привязку механизма рандомизации к его конкретной алгоритмической реализации.

Для усиления рандомизации в [3] предложено вместо фиксированного секретного вектора  $F$  использовать случайно выбираемый обратимый элемент  $V$  из КНАА, используемой в качестве алгебраического носителя, и вычислять подгоночный элемент  $S$  по формуле  $S = DGV$ . Однако, алгоритмическая реализация данного способа усиления рандомизации ЭЦП требует использования удвоенного проверочного уравнения, что приводит к уменьшению производительности процедур генерации и верификации подписи. Другим вариантом усиления рандомизации подписи является использование двух скрытых коммутативных групп таких, что элементы одной

из их являются некоммутативными с элементами другой. В алгоритмических реализациях этого механизма рандомизации, предложенных в [4, 5] для вычисления подгоночного элемента ЭЦП используется формула  $S = DPGF$ , где фиксированные векторы  $D$  и  $F$  используются как операнды левого и правого маскирующих умножений, а векторы  $P$  и  $G$  являются случайными представителями двух различных скрытых групп. Несмотря на одинаковый используемый способ рандомизации алгоритмы ЭЦП в статьях [4] и [5] являются существенно различными, например, в [5] впервые при построении алгебраических алгоритмов со скрытой группой, основанных на вычислительной трудности решения БССУ, в качестве секретного маскируемого множителя используется вектор, равный квадратному корню из единичного элемента КНАА.

В работе [7] дано обоснование использования трех различных коммутативных групп и вычисления вектора  $S$  по формуле  $S = DPGQF$ , где фиксированные векторы  $D$  и  $F$ , взаимно некоммутативные и некоммутативные с представителями каждой из трех скрытых групп,  $P$ ,  $G$  и  $Q$  являются случайными представителями трех различных скрытых групп, таких, что элементы каждой из них являются некоммутативными с элементами двух других скрытых групп. Переход от двух к трем скрытым группам привел при алгоритмической реализации к отказу от использования проверочного уравнения с операциями экспоненцирования вектора  $S$  и применения в проверочном уравнении значений хэш-функций, вычисляемых от  $S$  как способа обеспечения защищенности от подделки подписи путем решения проверочного уравнения относительно  $S$  как неизвестного вектора.

Представляет интерес идея усиления рандомизации [8], состоящая в использовании двух случайных выборок из одной скрытой группы, разделенных дополнительным фиксированным секретным множителем  $N$ , некоммутативным с представителями скрытой группы. Этот механизм рандомизации описывается формулой  $S = DGNHF$ , где векторы  $G$  и  $H$  — случайные представители скрытой группы, а фиксированные секретные множители  $D$ ,  $N$  и  $F$  попарно некоммутативны и некоммутативны с  $G$  и  $H$ . В данном варианте усиления рандомизации представляет интерес использование в качестве разделяющего множителя  $N$  некоторого нетривиального квадратного корня из единичного вектора. Другим развитием способа является использование трех случайных выборок из скрытой группы и формулы для вычисления подгоночного элемента подписи  $S$ , включающей два фиксированных разделяющих множителя.

#### СПИСОК ЛИТЕРАТУРЫ

1. Moldovyan N.A. Algebraic signature algorithms with a hidden group, based on hardness of solving systems of quadratic equations // *Quasigroups and Related Systems*. 2022, vol. 30, № 2. P. 287–298.
2. Moldovyan D.N. A new type of digital signature algorithms with a hidden group // *Computer Science Journal of Moldova*. 2023. V. 31. N. 1(91). P. 111–124. DOI: 10.56415/csjm.v31.06.
3. Moldovyan A.A. Complete signature randomization in an algebraic cryptoscheme with a hidden group // *Quasigroups and related systems*. 2024. Vol. 32. № 1. P. 95–108. DOI: 10.56415/qrs.v32.08.
4. Молдовян Н.А., Петренко А.С. Алгебраический алгоритм ЭЦП с двумя скрытыми группами // *Вопросы кибербезопасности*. 2024. № 6(64). С. 98–107. DOI: 10.21681/2311-3456-2024-6-98-107.
5. Захаров Д.В., Костина А.А., Морозова Е.В., Молдовян Д.Н. Алгоритм ЭЦП на алгебре матриц  $3 \times 3$ , использующий две скрытые группы // *Вопросы кибербезопасности*. 2025. № 3(67). С. 45–54. DOI: 10.21681/2311-3456-2025-3-45-54.
6. Moldovyan A.A., Moldovyan N.A. A method for enhancing randomization in algebraic signature algorithms on non-commutative algebras // *Quasigroups and related systems*. 2025. Vol. 33. № 1, pp.71–83. DOI: 10.56415/qrs.v33.06.
7. Moldovyan A.A., Moldovyan N.A. A method for enhancing randomization in algebraic signature algorithms on non-commutative algebras // *Quasigroups and related systems*. 2025. V. 33. N. 1. P.71–83. DOI: 10.56415/qrs.v33.06.
8. Молдовян А.А., Молдовян Д.Н., Костина А.А. Способ усиления рандомизации в постквантовых алгоритмах ЭЦП с секретной группой // *Информатика и автоматизация*. 2025. № 6. С. XXX–XXX. DOI: 10.15622/ia.XX.X.XX (в печати).

УДК 003.26

#### НОВЫЙ ТИП ПОСТКВАНТОВЫХ АЛГОРИТМОВ ЭЦП НА КОНЕЧНЫХ АЛГЕБРАХ МАТРИЦ

Морозова Елена Владимировна<sup>1</sup>, Михальченко Александра Викторовна<sup>2</sup>,

Молдовян Николай Андреевич<sup>1</sup>

<sup>1</sup> Государственный университет морского и речного флота имени адмирала С. О. Макарова  
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия

<sup>2</sup> Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)  
Профессора Попова ул., 5, Санкт-Петербург, 197022, Россия  
e-mails: lenmor@mail.ru, aleks.mihalchenko@gmail.com, nmold@mail.ru

**Аннотация.** Рассматривается парадигма построения постквантовых алгебраических алгоритмов ЭЦП, основанных на вычислительной трудности решения больших систем степенных уравнений (БССУ), отличающаяся вычислением открытого ключа с использованием двух операций возведения в степень в двух некоммутативных циклических группах, таких, что элементы одной из них некоммутативны с элементами другой. Задача решения БССУ возникает в рамках криптоанализа, состоящего в нахождении неизвестных степеней (элементов секретного ключа) путем сведения к задаче дискретного логарифмирования обычного типа. В качестве алгебраического носителя рассматриваемых алгоритмов ЭЦП рассматриваются конечные алгебры матриц различных размерностей  $k \times k$ . Для выполнения указанного криптоанализа используется возможность описаний элементов циклических групп, содержащихся в алгебрах матриц, через представителя группы и  $k$  скалярных значений. Дается оценка стойкости к квантовым атакам для различных вариантов реализации алгоритмов ЭЦП.

**Ключевые слова:** компьютерная безопасность; криптография; постквантовая криптография; цифровая подпись; конечные алгебры матриц; системы степенных уравнений.

## A NEW TYPE OF POST-QUANTUM SIGNATURE SCHEMES ON FINITE MATRIX ALGEBRAS

Morozova Elena<sup>1</sup>, Mikhilchenko Alexandra<sup>2</sup>, Moldovyan Nikolay<sup>1</sup>

<sup>1</sup> Admiral Makarov State University of Maritime and Inland Shipping

5/7 Dvinskaya St., St. Petersburg, 198035, Russia

<sup>2</sup> St. Petersburg State Electrotechnical University «LETI»

5 Professor Popov St, St. Petersburg, 197022, Russia

e-mails: lenmor@mail.ru, Aleks.mihalchenko@gmail.com, nmold@mail.ru.

**Abstract.** The article considers a paradigm for constructing post-quantum algebraic digital signature algorithms based on the computational difficulty of solving large systems of power equations (LSPE), characterized by calculating a public key using two exponentiation operations in two commutative cyclic groups such that the elements of one of them are non-commutative with the elements of the other. The problem of solving LSPE arises within the framework of cryptanalysis, which consists in finding unknown powers (elements of a secret key) by reducing to a discrete logarithm problem of the usual type. Finite algebras of matrices of various dimensions  $k \times k$  are considered as an algebraic carrier of the considered digital signature algorithms. To perform the specified cryptanalysis, the possibility of writing elements of cyclic groups contained in matrix algebras through a representative of the group and  $k$  scalar values is used. An assessment of the resistance to quantum attacks is given for various implementation options of the digital signature algorithms.

**Keywords:** computer security; cryptography; postquantum cryptography; digital signature; finite matrix algebras; systems of power equations.

Алгебраические алгоритмы ЭЦП [1], стойкость которых основана на вычислительной трудности решения больших систем степенных уравнений (БССУ), представляют собой новый тип алгоритмов многомерной криптографии [2, 3], которые перспективны в качестве двухключевых постквантовых криптосхем. В известных алгоритмах такого типа используется одна или более скрытых коммутативных групп [4, 5]. В настоящем сообщении обсуждается новая парадигма построения алгебраических алгоритмов ЭЦП, использующая вычислительную сложность решения БССУ. В качестве алгебраического носителя предполагается использование конечных алгебр матриц  $k \times k$ , в которых задаются в качестве известных параметров две матрицы  $G$  и  $J$ , генерирующие циклические группы достаточно большого порядка  $q$ , такие, что элементы одной из групп являются некоммутативными с элементами другой. В качестве секретного ключа выбираются два натуральных числа  $x$  и  $z$  ( $x < q$  и  $z < q$ ), а открытый ключ вычисляется в виде матрицы  $Y$  по формуле  $Y = G^x J^z$ . Легко показать, что при простом значении  $q$  различным парам  $(x, z)$  соответствуют различные матрицы  $Y$ . Вычисление секретного ключа по открытому при известных матрицах  $G$  и  $J$  можно трактовать как задачу спаренного дискретного логарифмирования в конечной алгебре матриц. Построение схемы ЭЦП, использующей открытый ключ вида  $Y = G^x J^z$ , выполняется в два этапа. На первом этапе разрабатывается многораундовая схема аутентификации с нулевым разглашением секрета, в которой в каждом из раундов включает три шага:

1. Доказывающий (удаленный абонент, подлинность которого устанавливается) генерирует случайный фиксатор  $R = GtJu$ , где  $x < q$  и  $z < q$  — случайные значения.

2. Проверяющий генерирует случайный равновероятный запрос в виде бита  $e$  и направляет  $e$  доказывающему.

3. Доказывающий вычисляет ответ в виде матрицы  $W$ , зависящей от  $Y$ ,  $R$  и  $e$ , и направляет  $W$  проверяющему. Последний с вероятностью 0.5 обнаруживает нарушителя.

На втором этапе указанная многораундовая схема аутентификации удаленных абонентов преобразуется по способу [6] в схему ЭЦП. Заметим, что аналогичное построение с использованием протокола аутентификации [7] известно для случая разработки схем ЭЦП на кодах, исправляющих ошибки [8].

Криптоанализ схемы ЭЦП с открытым ключом вида  $Y = G^x J^z$  показал, что секретный ключ  $(x, z)$  может быть вычислен путем нахождения матриц  $Y' = G^x$  и  $Y'' = J^z$  с последующим решением двух обычных задач дискретного логарифмирования. Нахождение матриц  $Y'$  и  $Y''$  осуществляется путем решения системы из  $k \times k$  степенных уравнений с  $2k$  неизвестными в поле, над которым задана алгебра матриц  $k \times k$ . Для получения 80-битной (256-битной) стойкости требуется использование конечной алгебры матриц с размером, определяемым значением  $k = 14$  ( $k = 100$ ), что приводит к построению алгоритмов ЭЦП с размером подписи равным  $\approx 30$  Кбайт ( $\approx 3$  Мбайт) при размере открытого ключа  $\approx 400$  байт ( $\approx 10$  Кбайт).

Аналогичные размеры подписи и открытого ключа получаются при построении схем ЭЦП путем преобразования протоколов аутентификации с нулевым разглашением секрета, использующих открытый ключа вида  $Y = \Phi(G^x)$ , где  $\Phi$  — функция автоморфного отображения алгебры матриц.

Для уменьшения размера ЭЦП предложены схемы с увеличенным размером открытого ключа в 3, 7 и 15 раз, за счет чего удалось уменьшить размер подписи в 2, 3 и 4 раза соответственно. Для более существенного сокращения размера ключа предложена постквантовая схема ЭЦП с открытым ключом вида  $Y = \Phi(G^x J^z)$ . По предварительным оценкам 80-битная (256-битная) стойкость модифицированной схемы ЭЦП достигается при размере подписи, равном  $\approx 20$  Кбайт ( $\approx 300$  Кбайт), и размере открытого ключа  $\approx 300$  байт ( $\approx 1$  Кбайт).

С учетом возможности сокращения размера ЭЦП для заданного уровня стойкости за счет приемлемого увеличения размера открытого ключа потенциально обеспечивается возможность построения постквантовых алгоритмов ЭЦП с приемлемыми для практического применения размерами открытого ключа и подписи. Представляет интерес реализация предложенных схем цифровой подписи с использованием в качестве алгебраического носителя конечных некоммутативных ассоциативных алгебр различных размерностей [9], что потенциально может обеспечить дополнительное уменьшение размеров открытого ключа и подписи.

Предлагаемые постквантовые схемы ЭЦП уступают по размерам открытого ключа и подписи алгебраическим алгоритмам со скрытой группой [10–13], однако превосходят по этим параметрам многие известные постквантовые алгоритмы ЭЦП, например, основанные на трудно обратимых отображениях с секретной лазейкой [14], на хеш-функциях [15] и на кодах, исправляющих ошибки [8].

#### СПИСОК ЛИТЕРАТУРЫ

1. Moldovyan D. № A new type of digital signature algorithms with a hidden group // *Computer Science Journal of Moldova*. 2023. V. 31. № 1(91). P. 111–124. doi:10.56415/csjm.v31.06.
2. Ding J., Petzoldt A., Schmidt D.S. Multivariate Cryptography // In: *Multivariate Public Key Cryptosystems. Advances in Information Security*. Springer, New York. 2020. V. 80. P. 7–23.
3. Ding J., Petzoldt A. Current State of Multivariate Cryptography // *IEEE Security and Privacy Magazine*. 2017, vol. 15, № 4, pp. 28–36.
4. Moldovyan A.A., Moldovyan N.A. A method for enhancing randomization in algebraic signature algorithms on non-commutative algebras // *Quasigroups and related systems*. 2025. Vol. 33. № 1, pp. 71–83. <https://doi.org/10.56415/qrs.v33.06>
5. Молдовьян Н.А., Петренко А.С. Алгебраический алгоритм ЭЦП с двумя скрытыми группами // *Вопросы кибербезопасности*. 2024. № 6(64). С. 98–107. DOI: 10.21681/2311-3456-2024-6-98-107.
6. Fiat A. and Shamir A. How to prove yourself: practical solutions to identification and signature problems. LNCS, 1987, vol. 263, pp. 186–194.
7. Stern J. A new identification scheme based on syndrome decoding. LNCS, 1994, vol. 773, pp. 13–21.
8. Vysotskaya V.V., Chizhov I. V. The security of the code-based signature scheme based on the Stern identification protocol // *Прикладная дискретная математика*. 2022. № 57. С. 67–90. DOI: 10.17223/20710410/57/5.
9. Moldovyan N.A. Unified Method for Defining Finite Associative Algebras of Arbitrary Even Dimensions // *Quasigroups and related systems*. 2018. V. 26. № 2. P. 263–270.
10. Захаров Д.В., Костина А.А., Морозова Е.В., Молдовьян Д.Н. Алгоритм ЭЦП на алгебре матриц  $3 \times 3$ , использующий две скрытые группы // *Вопросы кибербезопасности*. 2025. № 3(67). С. 45–54. DOI: 10.21681/2311-3456-2025-3-45-54.
11. Молдовьян Д.Н., Молдовьян А.А. Алгебраические алгоритмы ЭЦП, основанные на трудности решения систем уравнений // *Вопросы кибербезопасности*. 2022. № 2(48). С. 7–17. DOI: 10.21681/2311-3456-2022-2-7-17.
12. Duong M.T., Moldovyan D.N., Do B.V., Nguyen M.H., Post-quantum signature algorithms on non-commutative algebras, using difficulty of solving systems of quadratic equations // *Computer Standards and Interfaces*. 2023. V. 86. P. 103740. DOI: 10.1016/j.csi.2023.103740. ISSN 0920-5489.
13. Duong M.T., Moldovyan A.A., Moldovyan D.N., Nguyen M.H., Do T.-B. Structure of quaternion-type algebras and a post-quantum signature algorithm // *International Journal of Electrical and Computer Engineering*. 2024. V. 15. № 3. P. 2965–2976. DOI: 10.11591/ijece.v15i3.pp2965-2976.
14. Shuaiting Q., Wenbao H., Yifa L., and Luyao J. Construction of Extended Multivariate Public Key Cryptosystems // *International Journal of Network Security*. 2016. Vol. 18. № 1. P. 60–67.
15. Li L., Lu X., Wang K. Hash-based signature revisited. *Cybersecurity*. 2022, vol. 5. Article № 13. <https://doi.org/10.1186/s42400-022-00117-w>.

УДК 003.26

### СБАЛАНСИРОВАННЫЕ АЛГЕБРАИЧЕСКИЕ АЛГОРИТМЫ ЭЦП, ОСНОВАННЫЕ НА ВЫЧИСЛИТЕЛЬНОЙ ТРУДНОСТИ РЕШЕНИЯ БОЛЬШИХ СИСТЕМ УРАВНЕНИЙ

Морозова Елена Владимировна<sup>1</sup>, Щербаков Виктор Алексеевич<sup>2</sup>, Молдовьян Николай Андреевич<sup>2</sup>

<sup>1</sup> Государственный университет морского и речного флота имени адмирала С. О. Макарова  
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия

<sup>2</sup> СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия

e-mails: lenmor@mail.ru, victor.scerbacov@math.md, nmold@mail.ru

**Аннотация.** В данной работе предложен способ построения сбалансированных алгебраических схем ЭЦП, для которых уменьшается число потенциальных эквивалентных секретных ключей. Рассматриваются конкретные алгоритмические реализации и оценивается их стойкость. Показано, что разработанный способ может быть использован также и для построения переопределенных схем ЭЦП, в которых число уравнений, входящих в БССУ, больше числа неизвестных. В последнем случае размеры подписи и открытого ключа возрастают. Однако и в этом случае схемы ЭЦП остаются привлекательными как практичные постквантовые алгоритмы ЭЦП.

**Ключевые слова:** компьютерная безопасность; криптография; постквантовая криптография; цифровая подпись; конечные некоммутативные алгебры; системы степенных уравнений.

### BALANCED ALGEBRAIC SIGNATURE ALGORITHMS BASED ON THE COMPUTATIONAL HARDNESS OF SOLVING LARGE SYSTEMS OF EQUATIONS

Morozova Elena<sup>1</sup>, Shcherbacov Victor<sup>2</sup>, Moldovyan Nikolay<sup>2</sup>

<sup>1</sup> Admiral Makarov State University of Maritime and Inland Shipping  
5/7 Dvinskaya St., St. Petersburg, 198035, Russia

<sup>2</sup> St. Petersburg Federal Research Center of the Russian Academy of Sciences  
39 14th Line VO, St. Petersburg, 199178, Russia

e-mails: lenmor@mail.ru, victor.scerbacov@math.md, nmold@mail.ru.

**Abstract.** In this paper, a method for constructing balanced algebraic digital signature schemes is proposed. Specific algorithmic implementations are considered and their security is estimated. It is shown that the developed method can also be used to construct overdetermined digital signature schemes in which the number of equations included in the LSPE is greater than the number of unknowns. In the latter case, the sizes of the signature and the public key increase. However, in this case, digital signature schemes also remain attractive as practical post-quantum digital signature algorithms.

**Keywords:** computer security; cryptography; postquantum cryptography; digital signature; finite non-commutative algebras; systems of power equations.

Стойкость криптоалгоритмов с открытым ключом на трудно обратимых отображениях с секретной лазейкой основана на вычислительной трудности решения больших систем степенных уравнений (БССУ) [1, 2]. Постквантовые алгоритмы ЭЦП такого типа обладают малыми размерами подписи по сравнению с другими аналогами. Однако отнести их к практичным постквантовым схемам ЭЦП нельзя, поскольку в них размер открытого ключа является чрезвычайно большим.

Для построения практичных алгоритмов ЭЦП, основанных на вычислительной сложности решения БССУ, предложена парадигма алгебраических алгоритмов с одной или более скрытыми группами [3, 4],

Алгебраическим носителем в алгоритмах со скрытой группой является многомерная конечная некоммутативная алгебра (КНАА) с глобальной двухсторонней единицей. Открытый и секретный ключ включает некоторый набор векторов в качестве своих элементов. Элементы открытого ключа вычисляются по элементам секретного по формулам, которые задают систему степенных векторных уравнений, при решении которой выполняется ее сведение к БССУ в конечном поле, над которым задана используемая КНАА.

Решая данную БССУ, можно вычислить секретный ключ по значению открытого ключа. Данная атака называется прямой. Для обеспечения 80-битной (256-битной) стойкости к прямой атаке число уравнений в БССУ и число неизвестных должно быть не менее двадцати (ста) [2]. Вычислительная сложность решения зависит от степени уравнений и порядка поля, в котором задана БССУ, однако в существенно меньшей степени, чем от числа уравнений и неизвестных.

В алгоритмах на трудно обратимых отображениях БССУ задается в полях сравнительно малого порядка, имеющих размер от 4 до 32 бит. Это существенно контрастирует с алгоритмами ЭЦП со скрытой группой, в которых прямая атака связана с решением БССУ, заданной в конечных полях с размером порядка от 32 до 128 бит.

При этом при оценках стойкости предполагается слабая зависимость стойкости от значения порядка. Для увеличения числа степенных уравнений и числа неизвестных в алгоритмах последнего типа применяются КНАА большей размерности [5].

Частным видом КНАА являются конечные группы матриц. При этом для заданной размерности операция умножения в конечных алгебрах матриц имеет существенно более низкую вычислительную сложность по сравнению с другими видами КНАА.

Также важным является то, что для алгебр матриц известна формула для порядка мультипликативной группы, которая позволяет установить существующие значения порядка матриц, что используется при разработке алгоритмов ЭЦП со скрытой группой [6].

Для известных алгоритмов последнего типа число уравнений в БССУ существенно меньше числа неизвестных. Это соответствует случаю потенциального существования большого числа эквивалентных ключей и оцениванию сложности решения БССУ по числу уравнений. Для уменьшения числа потенциально возможных эквивалентных ключей представляет интерес разработка сбалансированных алгебраических алгоритмов со скрытой группой, т.е. алгоритмов, для которых БССУ включает число уравнений, равное числу неизвестных.

В данном сообщении рассматривается способ построения алгебраических алгоритмов со скрытой группой, который обеспечивает возможность разработки практичных постквантовых алгоритмов ЭЦП для различных уровней стойкости. Способ позволяет также разработать алгоритмы ЭЦП с переопределенными БССУ, в которых число уравнений превышает число неизвестных.

#### СПИСОК ЛИТЕРАТУРЫ

1. Ding J., Petzoldt A., Schmidt D.S. Multivariate Cryptography // In: Multivariate Public Key Cryptosystems. Advances in Information Security. Springer, New York. 2020. V. 80. P. 7-23.
2. Ding J., Petzoldt A. Current State of Multivariate Cryptography // IEEE Security and Privacy Magazine. 2017, vol. 15, № 4, pp. 28-36.
3. Moldovyan D.N. A new type of digital signature algorithms with a hidden group // Computer Science Journal of Moldova. 2023. V. 31. № 1(91). P. 111-124. doi:10.56415/csjm.v31.06.
4. Moldovyan A.A., Moldovyan N.A. A method for enhancing randomization in algebraic signature algorithms on non-commutative algebras // Quasigroups and related systems. 2025. Vol. 33. № 1, pp.71-83. <https://doi.org/10.56415/qrs.v33.06>
5. Молдовян Н.А., Петренко А.С. Алгебраический алгоритм ЭЦП с двумя скрытыми группами // Вопросы кибербезопасности. 2024. № 6(64). С. 98-107. DOI: 10.21681/2311-3456-2024-6-98-107.
6. Захаров Д.В., Костина А.А., Морозова Е.В., Молдовян Д.Н. Алгоритм ЭЦП на алгебре матриц  $3 \times 3$ , использующий две скрытые группы // Вопросы кибербезопасности. 2025. № 3(67). С. 45-54. DOI: 10.21681/2311-3456-2025-3-45-54.

УДК 004.056

**ПРИМЕНЕНИЕ ОНТОЛОГИЧЕСКОГО МОДЕЛИРОВАНИЯ ДЛЯ УПРАВЛЕНИЯ РИСКАМИ  
В ПРОМЫШЛЕННЫХ КИБЕРФИЗИЧЕСКИХ СИСТЕМАХ****Новикова Евгения Сергеевна, Мелешко Алексей Викторович**

СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия

e-mails: novikova@comsec.ru, meleshko.a@iiias.spb.su

**Аннотация.** При управлении рисками в промышленных киберфизических системах (КФС) необходимо учитывать разнородность различных требований, возникающих на разных этапах функционирования, что отличает решение данной задачи от управления рисками в традиционных информационных системах. Задача оценки рисков в КФС связана с решением таких проблемы, как децентрализация активов, высокий уровень неоднородности устройств Интернета вещей, а также наличия информации об уязвимостях в них. Возникает необходимость разработки подхода к управлению рисками информационной безопасности, который учитывает принципы поведения сложных систем, надежности и отказоустойчивости (безотказности), а также соответствия целям бизнес-процессов КФС. В работе предлагается онтологический подход к моделированию предметной области безопасности киберфизических систем для оценки рисков. Он связывает четыре основных компонента области, а именно киберфизическую систему, угрозы безопасности, последствия реализации угроз, последствия внедрения контрмер, что систематизировать знания о различных компонентах КФС и кибербезопасности и формализовать связи между ними. Последнее позволит автоматизировать процесс оценки рисков и выбор контрмер с учетом возможных последствий.

**Ключевые слова:** киберфизические системы; риски информационной безопасности; онтология; онтологическое моделирование; безопасность киберфизических систем.

**APPLICATION OF ONTOLOGICAL MODELING FOR RISK MANAGEMENT  
IN INDUSTRIAL CYBER-PHYSICAL SYSTEMS SECURITY****Novikova Evgenia, Meleshko Aleksei**

St. Petersburg Federal Research Center of the Russian Academy of Sciences

39 14th Line VO, St. Petersburg, 199178, Russia

e-mails: novikova@comsec.ru, meleshko.a@iiias.spb.su

**Abstract.** When managing risks in industrial cyber-physical systems (CFS), it is necessary to take into account the heterogeneity of various requirements that arise at different stages of operation, which distinguishes the solution of this problem from risk management in traditional information systems. The task of risk assessment in the CFS is related to solving problems such as asset decentralization, a high level of heterogeneity of Internet of Things devices, as well as the availability of information about vulnerabilities in them. There is a need to develop an approach to information security risk management that takes into account the principles of behavior of complex systems, reliability and fault tolerance, as well as compliance with the goals of the CFS business processes. The paper proposes an ontological approach to modeling the security domain of cyber physical systems for risk assessment. It connects four main components of the field, namely the cyber-physical system, security threats, the consequences of threats, the consequences of implementing countermeasures, which systematize knowledge about the various components of the CFS and cybersecurity and formalize the links between them. The latter will automate the risk assessment process and the selection of countermeasures, taking into account possible consequences.

**Keywords:** cyber physical systems; information security risks; ontology; ontological modeling; security of cyber physical systems.

Сегодня, киберфизические системы (КФС) плотно интегрированы во все критически важные и социально значимые инфраструктуры, такие как горнодобывающие и химические заводы, транспортные системы, системы водоснабжения и т.д. Сложность КФС заключается в их непосредственном взаимодействии с физическими процессами и окружающей средой, они сочетают в себе элементы контроля и воздействия на окружающую физическую среду, а также элементы обработки полученных данных о ней. Кроме того, такие элементы КФС как датчики или исполнительные механизмы могут располагать в незащищенном окружении, что увеличивает риск их компрометации со стороны злоумышленников.

Для построение эффективной системы управления информационными рисками необходима систематизация знаний о возможных угрозах безопасности КФС, последствий от угроз и о существующих мерах противодействия данным угрозам. Кроме того, к КФС предъявляется множество различных требований, которые следует учитывать при разработке системы знаний о ее безопасности и которые меняются на различных этапах описании ее жизненного цикла [1].

Одним из подходов к такой систематизации знаний предметной области является онтологическое моделирование. Такое моделирование активно используется исследователями при описании различных информационных угроз и атак на информационные системы.



Онтологии организуют разнородные данные кибербезопасности таким образом, что появляется возможность извлекать новые концепции и модели поведения, например, измерять уровень риска системы или генерировать показатели защищенности для информационных систем. систем поддержки принятия решений.

Например, в [2] предложена модель безопасности приложений, в основе которого лежит онтология, которые описывает такие сущности как сетевые настройки, конфигурации приложений, методы и инструменты тестирования, а также показатели безопасности, которые в совокупности позволяют оценить степень защищенности критически важного приложения в контексте его инфраструктуры размещения.

Онтология STIX [3] описывает такие сущности информационной безопасности как атака, кампания, инструменты, уязвимости, атакующие и т.д., и определяет связи между ними. Ее применение позволяют по наблюдаемым событиям, используемым атакующим техникам и инструментами определить потенциальных злоумышленников, а их действия связать в единую кампанию.

В [4] предложена онтология, которая связывает наблюдаемые аномалии и риски, определяемые для различных устройств. В [5, 6] представлены онтологии, которая предназначены для определения метрик информационной безопасности с учетом контекста их применения.

В [5] контекст определяет через такие понятия как человеческий фактор, время, местоположение и вычислительные особенности, вероятность, критичность и цель бизнес-процессов, для которых вычисляются данные метрики.

Таким образом, в научной литературе представлены разнообразные онтологии для управления информационной безопасностью, однако отсутствует комплексный подход, который связывает описание разнородных киберфизических систем, наблюдаемые аномалии, включая инциденты безопасности, расчет рисков и выбор контрмер в зависимости от последствий их реализаций.

Целью данной работы является:

1. Определение и разработка единой обобщенной модели информационной безопасности КФС, которая использует онтологические концепции и принципы для описания сложной динамической природы системы.
2. Разработка системы метрик и показателей риска, связанных с ресурсами КФС и наблюдаемыми событиями безопасности.
3. Разработка концептуальной основы для описания контрмер с учетом особенностей технологического процесса, общих бизнес-целей предприятия и возможными последствиями их применения.

Разрабатываемая онтология должна давать формальную спецификацию основных элементов предметной области и включать в себя описание всех отношений между этими элементами. Таким образом наглядно систематизируются все угрозы для КФС и их последствия. Кроме того, онтология позволяет проводить формализацию знаний о предметной области безопасности КФС, а также упрощает восприятие информации о ней для человека.

В данной работе раскрываются аспекты применения подхода онтологического моделирования предметной области безопасности КФС, в частности обсуждаются вопросы определения различных уровней моделирования: общие концепты высокого уровня абстракции, концепты среднего уровня, и концепты нижнего уровня, которым относятся классы, детализирующие особенности классов среднего уровня, например, сетевые интерфейсы передачи данных, особенности аппаратного обеспечения и т.д.

Также описываются основные высокоуровневые компоненты разрабатываемой онтологии: описание КФС, угрозы безопасности КФС, последствия от реализации угроз, а также влияние контрмер на выявленные угрозы, оценивается возможность использования уже разработанных онтологий, таких как STIX и онтологии COIoT для моделирования Интернета Вещей [7, 8].

Таким образом, в данной работе был предложен подход к онтологическому моделированию области безопасности киберфизических систем. Онтология объединяет в себе такие компоненты как КФС, угрозы безопасности, последствия реализации угроз и контрмеры. В рамках онтологии наглядно строятся и систематизируются взаимосвязи между всеми компонентами, что позволяет адекватно оценить уровень безопасности КФС и оперативно выбирать контрмеры в случае наблюдаемых аномалий.

*Исследование выполнено за счет гранта Российского научного фонда № 23-11-20024.*

#### СПИСОК ЛИТЕРАТУРЫ

1. Tebbe C., Niemann K.-H., A. Fay. Ontology and life cycle of knowledge for ICS security assessments. 2016. DOI: 10.14236/ewic/ICS2016.5.
2. Mozzaquatro, B.A.; Agostinho, C.; Goncalves, D.; Martins, J.; Jardim-Goncalves, R. An Ontology-Based Cybersecurity Framework for the Internet of Things. *Sensors* 2018, *18*, 3053. <https://doi.org/10.3390/s18093053>.
3. Онтология STIX. URL: <https://oasis-open.github.io/cti-documentation/stix/intro> (дата обращения 20.08.2025).
4. Sánchez-Zas C., Villagrà V.A., Vega-Barbas M., Larriva-Novo X., Moreno J. I., Berrocal J. Ontology-based approach to real-time risk management and cyber-situational awareness // *Future Generation Computer Systems*, 2023. Vol. 141, p. 462-472.
5. Khaleghi M., Reza Aref M., and Rasti M. 2022. Context-Aware Ontology-based Security Measurement Model. *J. Inf. Secur. Appl.* 67, C (Jun 2022). <https://doi.org/10.1016/j.jisa.2022.103199>.
6. E. Doynikova, A. Fedorchenko, and I. Kotenko, «Ontology of Metrics for Cyber Security Assessment», in *Proceedings of the 14th International Conference on Availability, Reliability and Security, ARES '19*, Canterbury, UK, Article No. 52, pp. 1-8, August 26–29, 2019.
7. Tayur, V.M.; Suchithra, R. A comprehensive ontology for internet of things (COIoT). In *Proceedings of the 2019 Second International Conference on Advanced Computational and Communication Paradigms (ICACCP)*, Gangtok, India, 25–28 February 2019; pp. 1–6.
8. Qaswar, F.; Rahmah, M.; Raza, M.A.; Noraziah, A.; Alkazemi, B.; Fauziah, Z.; Hassan, M.K.A.; Sharaf, A. Applications of Ontology in the Internet of Things: A Systematic Analysis. *Electronics* 2023, *12*, 111. <https://doi.org/10.3390/electronics12010111>.

УДК 004.056

**МИНИМАЛЬНО ДОСТАТОЧНЫЕ ТРЕБОВАНИЯ ЗАЩИЩЕННОСТИ СИСТЕМ ОБРАБОТКИ И ХРАНЕНИЯ БОЛЬШИХ ДАННЫХ****Полтавцева Мария Анатольевна, Александрова Елена Борисовна, Ворошин Евгений Александрович**

Санкт-Петербургский политехнический университет Петра Великого

Политехническая ул., 29, Санкт-Петербург, 195251, Россия

e-mails: poltavtseva@ibks.spbstu.ru, helen@ibks.spbstu.ru, voroshin\_ea@spbstu.ru

**Аннотация.** Рассматриваются минимально достаточные требования защищенности в отношении гетерогенных систем обработки и хранения больших данных, обусловленные специфическими особенностями объектов защиты.

**Ключевые слова:** информационная безопасность; большие данные; гетерогенные системы; распределенные системы; требования безопасности.

**MINIMUM SECURITY REQUIREMENTS FOR BIG DATA PROCESSING AND STORAGE SYSTEMS****Poltavtseva Maria, Aleksandrova Elena, Voroshin Evgenii**

Peter the Great St. Petersburg Polytechnic University

29 Polytechnicheskaya st., St. Petersburg, 195251, Russia

e-mails: poltavtseva@ibks.spbstu.ru, helen@ibks.spbstu.ru, voroshin\_ea@spbstu.ru

**Abstract.** The minimally security requirements for heterogeneous big data processing and storage systems due to the specific features of security facilities are considered.

**Keywords:** information security; big data; heterogeneous systems; distributed systems; security requirements.

Современный уровень цифровизации предприятий и организаций различных сфер деятельности приводит обуславливает интеграцию информационных систем и автоматизированных систем различного назначения (включая промышленные системы, системы цифровых двойников и иные). Возникают сложные экосистемы управления данными, которые содержат также значимое число конфиденциальной информации. К такого рода сведениям относятся как персональные данные, так и данные о деятельности организации, принадлежащих ей объектам и оборудованию. В то же время в России, как и в целом мире, предприятия малого и среднего бизнеса все больше становятся целью компьютерных атак. Количество утечек данных, с учетом объема попадающих в руки злоумышленников сведений, становится все больше. Зачастую атаки проводятся с участием внутреннего нарушителя или путем дискредитации учетной записи сотрудника.

В этих условиях цифровые экосистемы больших данных являются привлекательно целью для злоумышленника. В то же время, гетерогенные экосистемы больших данных, представляющие собой интеграцию большого числа продуктов и сервисов, включая, в своей основе, СУБД различного типа, для решения общих задач над массивом данных и/или его отдельными элементами, обладают рядом уязвимостей, свойственных только этому классу систем, и не присущих традиционным СУБД. Они обусловлены гетерогенностью используемых инструментов управления данными и распределенном (в том числе, географически и организационно) характере работы указанных систем [1, 2]. Это, в первую очередь:

- разнородная не согласованная система контроля доступа;
- большое число пользователей с привилегированным доступом;
- как правило, высокая степень доверия между системами.

Анализ законодательства в области информационной безопасности, в частности ФЗ №152 «О персональных данных» и его подзаконных актов (в частности, приказ ФСТЭК России № 21 от 18.02.2013), |ФЗ № 187 «О безопасности критической информационной инфраструктуры Российской Федерации» с соответствующими нормативно-правовыми актами, а также требований по обеспечению безопасности в государственных информационных системах позволяет выделить области требований, реализация которых затрагивает данные особенности. Это, в частности, сквозные и согласованные в отношении всех инструментов (включенных в систему обработки данных) управление и мониторинг доступа к данным, минимизация прав доступа, защита и согласованный сбор данных об информационных потоках для выявления событий безопасности. Реализация данных требований на уровне отдельного инструмента обработки данных является более простой задачей, тогда как исполнение их над всей гетерогенной распределенной экосистемой обработки и хранения больших данных является сложно научно-технической задачей [1, 3]. Учитывая выделенные ранее особенности рассматриваемого класса объектов защиты, сформулируем минимально достаточные требования для обеспечения защищенности гетерогенной распределенной системы обработки и хранения больших данных.

Первым требованием является согласованное управление доступом к данным над всей гетерогенной распределенной системы обработки и хранения данных. Особенностью данного класса систем является использование одних и тех же данных в рамках сложного жизненного цикла в различных компонентах системы. Допустим, существует пользователь  $u_1$  который имеет доступ к данным через доступ к инструменту (СУБД)  $i_1$  а также, в силу совмещения обязанностей или особенности должности — к тем же данным на инструменте  $i_2$ . Примером такого пользователя может служить администратор, имеющий доступ к данным кадрового и/или

бухгалтерского учета объекта, а также к данным полученным с удаленного производственного объекта (в частности, о рабочих сменах). В этом случае если на инструменте  $i_1$  пользователю к конкретным данным  $d$  предоставлен набор прав  $p_1$  а на инструменте  $i_2$ , на котором также обрабатываются или хранятся данные  $d$ , набор прав -  $p_2$ , случай, когда множества  $p_1$  и  $p_2$  не равны показывает либо ситуацию, когда пользователю предоставлено недостаточно прав (что маловероятно в условиях устоявшихся бизнес-процессов), либо ситуацию избыточного предоставления прав и возможности утечки конфиденциальных данных. Такая ситуация может возникнуть в так как инструменты в рамках систем обработки и хранения больших данных не зависимы, как правило обладают высокой степенью доверия к друг другу, а права доступа настраиваются на каждом инструменте отдельно. Отметим, что на практике такие ситуации являются не только сложно выявляемыми, так как в современных инфраструктурах обнаруживаются только вручную, но и зачастую сложно преодолимыми в силу различной грануляции объектов данных [2]. На практике требование может быть сформулировано следующим образом: *пользователь должен иметь одинаковый набор прав доступа к данным вне зависимости от их структуризации в конкретных инструментах обработки и хранения данных*. Вторым требованием становится минимизация прав доступа к объектам данных в гетерогенных распределенных системах обработки и хранения данных. В случае превышения минимального доступа нарушается принцип минимизации привилегий. Однако такая ситуация может возникнуть в силу двух обстоятельств. Во-первых, в силу ошибок администрирования из-за высокой степени доверия между инструментами обработки и хранения данных, когда администратор одной системы получает доступ к данным другой, через подконтрольные ему запросы. В этом случае правило безопасности можно сформулировать следующим образом: *доступ к данным внутри каждой системы со стороны сторонних инструментов должен регулироваться правами пользователей или процессов, со стороны которых осуществляется данный доступ*, а не совокупными правами инструмента.

Во-вторых, в силу различной грануляции данных на различных инструментах. Так, в примере приведенном выше, администратор может получить минимально необходимый набор прав в отношении персональных данных работника в реляционном сервере с кадровыми и финансовыми данными, однако данные приходящие с объекта, и также содержащие персональную информацию, включая информацию о перемещениях и здоровье (в силу медицинского контроля состояния работника) могут записываться отдельными документами в документно-ориентированное хранилище или хранилище типа ключ — значение, и тогда доступ технически может быть настроен только к записи целиком. В результате администратор получает, с одной стороны, одинаковый набор прав доступа в отношении необходимых ему данных, но также имеет доступ к иным конфиденциальным данным, который не может быть просто предотвращен в текущей технологической инфраструктуре. В данном случае на практике требование безопасности формулируется следующим образом: *пользователю должен быть предоставлен доступ только к тем данным, которые необходимы ему для исполнения своих функций, либо к не конфиденциальным данным, вне зависимости от грануляции объектов данных*. В случае описанного примера данные с объекта должны быть разделены до записи в промежуточное хранилище, к которому пользователю предоставляется доступ. Это требование справедливо и для администраторов систем, которые не должны иметь прямого доступа к данным, обрабатываемым в администрируемых ими системах, если эти данные являются конфиденциальными. Сегодня это также технологически сложная задача решаемая либо специализированными решениями со сквозным шифрованием [4], либо более специфическими способами маскирования [5].

Третьим требованием становится обеспечение мониторинга процессов обработки данных, так как в условиях распределенной масштабной инфраструктуры автоматизированный единый мониторинг является единственным способом обеспечения контроля реализации приведенных требований. В основу такого мониторинга может быть положена система сбора данных и моделирования процессов в системах больших данных [2] или иные решения по распределенному мониторингу, разработанные для соответствующей инфраструктуры. С формальной точки зрения *все потоки данных в системе обработки и хранения больших данных должны быть отслеживаемы на всех уровнях грануляции* (как внутри инструментов обработки, что обычно реализуется их встроенным функционалом, так и между ними) *с учетом источников и получателей данных и определенных для них прав доступа*. На практическом уровне требование безопасности может быть сформулировано как: обеспечение защищенного автоматизированного мониторинга процессов обработки данных в системах обработки и хранения больших данных.

Исполнение приведенных требований, с одной стороны, обеспечивает реализацию формальных требований на уровне распределенной инфраструктуры, а с другой, в совокупности с известными требованиями в отношении гомогенных систем обработки и хранения данных, минимально необходимы и достаточны для обеспечения защищенности с учетом особенностей объекта.

#### СПИСОК ЛИТЕРАТУРЫ

1. Dritsas E., Trigka M. A Survey on Database Systems in the Big Data Era: Architectures, Performance, and Open Challenges //IEEE Access. T. 13. 2025. С. 95068-95084. DOI: 10.1109/ACCESS.2025.3572059.
2. Poltavtseva M. A., Kalinin M. O. Access control analysis in heterogeneous big data management systems //Programming and Computer Software. T. 50. № 7. 2024. С. 549-558.
3. Ren Y. et al. PolyStore: exploiting combined capabilities of heterogeneous storage //Proceedings of the 23rd USENIX Conference on File and Storage Technologies. Santa Clara, CA, USA, 2025. С. 539-555.
4. Shi G. et al. Efficient cryptanalysis of an encrypted database supporting data interoperability //The VLDB Journal. T. 33. № 5. 2024. С. 1357-1375.
5. Bosnjak M., Redzepagic J., Zgrablic L. DATA MASKING AND TOKENISATION //Proceedings of the 35th DAAAM International Symposium. T. 35. 2024. С.0183-01902024. DOI: 10.2507/35th.daaam.proceedings.024.

УДК 004.056

**МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БАЗ ДАННЫХ****Пучков Владимир Викторович, Виткова Лидия Андреевна**

СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия

e-mails: puchkov-81@bk.ru, lidia.vitkova@yandex.ru

**Аннотация.** В современном информационном пространстве объемы информационных массивов имеют тенденцию постоянного динамического роста. И проблема «утечки» информации в том числе и персональных данных является одним из приоритетных направлений защиты при обеспечении информационной безопасности баз данных. В работе рассматриваются специфические угрозы безопасности массивам данных, а также технологии, применяемые для обеспечения информационной безопасности современных систем управления базами данных. Проведен анализ применяемых средств защиты в СУБД Российской разработки. Особое внимание уделяется технологии «маскирования» данных, что в сфере ужесточения требований Российского законодательства в исполнении 152-ФЗ [1] особенно актуально.

**Ключевые слова:** маскирование данных; СУБД — системы управления базами данных; информационная безопасность; защита; автоматизация поиска.

**DATABASE SECURITY METHODS****Puchkov Vladimir, Vitkova Lidia**

St. Petersburg Federal Research Center of the Russian Academy of Sciences

39 14th Line VO, St. Petersburg, 199178, Russia

e-mails: puchkov-81@bk.ru, lidia.vitkova@yandex.ru

**Abstract.** In the modern information space, the volume of information arrays tends to constantly grow dynamically. And the problem of «leakage» of information, including personal data, is one of the priority areas of protection while ensuring the information security of databases. The paper considers specific threats to the security of data arrays, as well as technologies used to ensure the information security of modern database management systems. The analysis of the applied protection tools in the Russian-designed DBMS is carried out. Special attention is paid to the technology of «masking» data, which is especially relevant in the field of tightening the requirements of Russian legislation in compliance with 152-FZ [1].

**Keywords:** data masking; database management systems; information security; protection; search automation.

Обеспечение безопасности хранилищ данных, обеспечение условий хранения конфиденциальной информации в современных условиях является приоритетным для организаций различных форм собственности. Этот вопрос актуален для коммерческих решений и для госпредприятий.

Сегмент обеспечения информационной безопасности баз данных в разрезе построения системы защиты информации организации является важным и даже критическим, если рассматривать этот вопрос в рамках исполнения 152-ФЗ. В настоящее время для обеспечения безопасности СУБД имеется достаточно большое количество наложенных и встроенных средств защиты информации.

Нужно отметить, что на данный момент рынок СУБД российской разработки как никогда находится на взлете. В 2024 году он составил 35 млрд. рублей, а, по некоторым прогнозам, через пять лет может вырасти до 66 млрд. рублей [2]. Такой эффект является следствием ухода с рынка иностранных вендоров и исполнения Указа Президента РФ от 30.03.2022 № 166 (ред. от 07.04.2025) «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации». Реляционные системы управления базами данных российской разработки на территории РФ в обязательном порядке обеспечивают управление доступом к информации, хранящейся в базах данных. Различия в системах выпускаемых различными вендорами заключаются в различных подходах к построению архитектуры безопасности, процедурной реализации, применении open-source решений или разработке собственных модулей безопасности.

Ниже приведен перечень наиболее часто рассматриваемого функционала безопасности, применяемого в разработках современных российских СУБД:

- сокрытие информации в файлах данных СУБД;
- сокрытие хранимых процедур и функций;
- защита от SQL-атак;
- маскирование данных;
- наличие отказоустойчивого кластера;
- проверка целостности данных;
- аудит событий;
- ограничение прав суперпользователя;
- аутентификация;
- применение расширенных политик безопасности;
- шифрование данных (при хранении и передаче);

- шифрование паролей;
- восстановление данных;
- очистка памяти (без возможности восстановления данных);
- способы хранения логов событий безопасности.

В процессе исследования были рассмотрены следующие СУБД Российского производства: Рэд База Данных, Postgres Pro Enterprise, Jatoba Enterprise Certified, Tantor Certified PostgreSQL SE, Platform V Pangolin SE, Arenadata Prosperity (Proxima DB SE). В целом данные СУБД сертифицированные по 4-му уровню доверия ФСТЭК обладают достаточно схожим функционалом в области обеспечения безопасности. Однако хочется отметить, что в некоторых рассматриваемых СУБД указанный выше функционал безопасности не обеспечивается встроенными средствами защиты и требует доработки специалистами по информационной безопасности. Среди таких параметров безопасности можно отметить: защита от SQL- инъекций, шифрование паролей, маскирование данных и сокрытие хранимых процедур и триггеров. Такой подход создает дополнительные уязвимости и может стать причиной проникновения злоумышленников в хранилище данных. Автоматизация поиска и детектирования информации, подлежащей маскированию, является важным этапом по обеспечению безопасности персональных данных. Одним из направлений дальнейших исследований можно отметить разработку алгоритмов и методик по выявлению конфиденциальной информации с целью ее дальнейшего маскирования [3].

#### СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ (последняя редакция) [Электронный ресурс] // URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_61801/](https://www.consultant.ru/document/cons_doc_LAW_61801/) (дата обращения: 25.08.2025).
2. Российские СУБД: обзор альтернатив Oracle, Microsoft и IBM // Тренды 2025 [Электронный ресурс] // URL: [https://www.anti-malware.ru/analytics/Market\\_Analysis/Russian-database-management-systems-2025#part3](https://www.anti-malware.ru/analytics/Market_Analysis/Russian-database-management-systems-2025#part3) (дата обращения: 25.08.2025).
3. Лось, В. П. РАЗРАБОТКА ресурсно-эффективной техноЛОГИИ динамическоГО маскированиЯ конфиденциальнОЙ ИНФОРМАЦИИ в реляционных базах данных / В. П. Лось, Д. Д. Маланьин // Информация и безопасность. 2023. Т. 26, № 4. С. 551-560. DOI 10.36622/VSTU.2023.4.26.007. EDN AXNEFI.

УДК 004.056

#### ЭТИЧЕСКИЙ ХАКИНГ В СТРАТЕГИИ КИБЕРБЕЗОПАСНОСТИ

**Рябов Геннадий Анатольевич, Яровой Роберт Владимирович**

Военная академия связи им. Маршала Советского Союза С. М. Буденного  
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия  
e-mails: grif999@mail.ru, Nadzar@yandex.ru

**Аннотация.** В тезисе раскрываются концептуальные основы, методы, юридические ограничения и потенциальные конфликты, возникающие при привлечении белых хакеров. Подчеркивается необходимость нормативной ясности, технологической гибкости и соблюдения этических стандартов.

**Ключевые слова:** этический хакинг; кибербезопасность; белые хакеры; тестирование на проникновение; информационная защита; уязвимости; юридические риски.

#### ETHICAL HACKING IN CYBERSECURITY STRATEGY

**Ryabov Gennady, Yarovoy Robert**

Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny  
3 Tikhoretsky Av, St. Petersburg, 194064, Russia  
e-mails: grif999@mail.ru, Nadzar@yandex.ru

**Abstract.** The thesis explores the conceptual underpinnings, methods, legal constraints, and potential conflicts that arise when engaging white hat hackers. It emphasizes the need for regulatory clarity, technological flexibility, and ethical standards.

**Keywords:** ethical hacking; cybersecurity; white hat hackers; penetration testing; information security; vulnerabilities; legal risks.

Этический хакинг, позиционируемый как легализованная форма наступательной кибербезопасности, позволяет организациям обнаруживать уязвимости до их эксплуатации. В отличие от противоправных вмешательств, белый хакинг осуществляется по согласованию с владельцами инфраструктуры, в рамках строго очерченного юридического и этического поля [1, 2].

Ключевыми составляющими этого подхода являются:

- согласие и предварительная договорённость;
- конфиденциальность всех полученных данных;
- отчётность и прозрачность действий специалистов;
- ограничение по целям, методам и масштабу тестирования.

Различают три модели тестирования: white box, при которой специалист получает полный доступ к внутренней архитектуре; black box, имитирующую действия внешнего злоумышленника; и gray box, сочетающую

оба подхода. Инструментарий включает Metasploit, Nmap, Wireshark и иные среды, направленные на выявление системных и сетевых уязвимостей [3, 4].

Однако эффективность этического хакинга сопряжена с вызовами: от рисков юридических недоразумений в случае нечетко оформленных соглашений — до моральных дилемм и технической сложности анализа многоуровневых ИТ-систем. Имеются прецеденты, где несогласованность документации приводила к спорам, несмотря на добросовестность исполнителя.

Значительное внимание уделяется правовому контексту: актуальность приобретают локальные нормы, международные стандарты (например, ISO/IEC 27001), соглашения о неразглашении, регламенты действий. Наряду с этим обсуждается необходимость повышения квалификации специалистов и институционального признания профессии через сертификацию и образовательные инициативы [5].

Таким образом, этический хакинг выходит за рамки технологического эксперимента, превращаясь в форму институционализированного противодействия угрозам. Его развитие сопряжено с выработкой правовых механизмов, повышением прозрачности процедур и формированием доверия между участниками цифровой экосистемы. В условиях возрастающей сложности атак и нормативной неопределённости именно белые хакеры становятся связующим звеном между инфраструктурой и её уязвимостями. Их деятельность — это не демонстрация силы, а акт ответственности в архитектуре цифровой безопасности.

#### СПИСОК ЛИТЕРАТУРЫ

1. Дэниел Г.Г. Этический хакинг. Практическое руководство по взлому // Питер. 2022. № 15 (514). С. 23-27.
2. Яровой Р.В., Рябов Г.А., Карганов В.В. Кибербезопасность в мире инфотелекоммуникаций: вызовы и стратегии защиты // инновационная деятельность в Вооруженных Силах Российской Федерации. 2023. С. 373-377.
3. Роберт В.Б. Освоение Kali Linux для расширенного тестирования на проникновение // [Электронный ресурс]. URL <https://docs.yandex.ru/docs/view?tm=1721305945&tld=ru&lang=en&name=books-library.net-> (дата обращения 18.07.2024).
4. Яровой Р.В., Кривоногова Е.В., Рябов Г.А. Атаки на веб-приложения: определение, типы и профилактика // Тенденции развития науки и образования. 2023. № 101-4. С. 96-98.
5. Хакерская\_этика. [Электронный ресурс]. URL [https://ru.wikipedia.org/wiki/Хакерская\\_этика](https://ru.wikipedia.org/wiki/Хакерская_этика) (дата обращения 18.07.2024).

УДК 004.8

#### АНАЛИЗ ПРИМЕНЕНИЯ АВТОЭНКODЕРОВ ДЛЯ ПОВЫШЕНИЯ ТОЧНОСТИ КЛАССИФИКАЦИИ ИЗОБРАЖЕНИЙ

Садовников Владимир Евгеньевич, Саенко Игорь Борисович

СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия

e-mails: bladimir1998@mail.ru, ibsaen@comsec.spb.ru

**Аннотация.** Автоэнкодеры — это нейронные сети для безучительного обучения компактных представлений данных, основанные на принципе сжатия в латентное пространство и последующего восстановления. Существует множество модификаций — от вариационных и шумоподавляющих до сверточных, рекуррентных и гибридных моделей, таких как VAE-GAN, — каждая из которых расширяет функциональность автоэнкодеров в задачах генерации, анализа и интерпретации данных. Они находят применение в обработке изображений, текстов, временных рядов и мультимодальных системах, играя ключевую роль в современном глубоком обучении.

**Ключевые слова:** автоэнкодер; глубокое обучение; искусственный интеллект; машинное обучение; нейронные сети.

#### ANALYSIS OF THE USE OF AUTOENCODERS TO IMPROVE ACCURACY IMAGE CLASSIFICATIONS

Sadovnikov Vladimir, Saenko Igor

St. Petersburg Federal Research Center Russian Academy of Sciences

39 14th Line VO, St. Petersburg, 199178, Russia

e-mails: bladimir1998@mail.ru, ibsaen@comsec.spb.ru

**Abstract.** Autoencoders are neural networks for training-free learning of compact data representations based on the principle of compression into latent space and subsequent recovery. There are many modifications, from variational and noise-canceling models to convolutional, recurrent, and hybrid models such as VAE-GAN, each of which extends the functionality of autoencoders in data generation, analysis, and interpretation tasks. They find applications in image processing, text processing, time series, and multimodal systems, playing a key role in modern deep learning.

**Keywords:** autoencoder; deep learning; artificial intelligence; machine learning; neural networks.

Автоэнкодеры — это нейронные сети для безучительного обучения компактных представлений данных, состоящие из энкодера, сжимающего вход в латентное пространство, и декодера, восстанавливающего исходные данные. Основная цель — минимизировать ошибку реконструкции, что позволяет выявлять ключевые признаки и структуру [1].

Простейшие автоэнкодеры используют полносвязные слои и применяются для сжатия и предобработки данных. Разреженные автоэнкодеры вводят регуляризацию активаций, повышая интерпретируемость, а шумоподавляющие обучаются восстанавливать чистые данные из зашумленных, обеспечивая устойчивость к искажениям [2].

Вариационные автоэнкодеры (VAE) моделируют латентные переменные как распределения, позволяя генерировать новые данные; их модификация,  $\beta$ -VAE, способствует дисэнганглированию — разделению независимых факторов, таких как форма и цвет [3].

Для изображений используются сверточные автоэнкодеры, сохраняющие пространственную структуру, а для последовательных данных — рекуррентные (LSTM/GRU) или трансформерные, как в BERT, эффективно моделирующие временные и контекстные зависимости [4].

Семантические автоэнкодеры фокусируются на сохранении смысла, а не пикселей, используя внешние знания, например, эмбединги слов. Стилизованные автоэнкодеры разделяют контент и стиль, что полезно в задачах переноса стиля.

Гибридные модели, такие как VAE-GAN, сочетают структурированное латентное пространство VAE с высоким качеством генерации GAN. Автоэнкодеры с пропускными связями позволяют строить более глубокие и стабильные сети, аналогично ResNet. Контрактирующие автоэнкодеры регуляризуют чувствительность латентного кода к изменениям входа, повышая робастность [5].

Мультимодальные автоэнкодеры обрабатывают разные типы данных — текст, изображения, звук — и строят общее латентное пространство для кросс-модального поиска и синтеза.

Совокупность этих модификаций расширяет применение автоэнкодеров от очистки и сжатия данных до генерации, анализа аномалий и создания интерпретируемых моделей в современном глубоком обучении [6].

#### СПИСОК ЛИТЕРАТУРЫ

1. Qi G-J, Luo J. Small data challenges in big data era: a survey of recent progress on unsupervised and semi supervised methods. *IEEE Trans Pattern Anal Mach Intell.* № 44(4), 2020, P. 2168–2187.
2. Pinaya WHL, Vieira S, Garcia-Dias R, Mechelli A. Autoencoders. *Machine Learning.* Elsevier, 2020, pp 193–208.
3. Qian J, Song Z, Yao Y, Zhu Z, Zhang X. A review on autoencoder based representation learning for fault detection and diagnosis in industrial processes. *Chemom Intell Lab Syst* 231:104711, 2022.
4. Bank D., Koenigstein N., Giryas R. Autoencoders. In *Machine learning for data science handbook: data mining and knowledge discovery handbook*, 2023, pp 353–374.
5. Wang S, Wang X, Zhang L, Zhong Y. Auto-ad: autonomous hyperspectral anomaly detection network based on fully convolutional autoencoder. *IEEE Trans Geosci Remote Sens* № 60, 2021, P. 1–14.
6. Eddahmani I, Pham C-H, Napoléon T, Badoc I, Fouefack J-R, El-Bouz M. Unsupervised learning of disentangled representation via auto-encoding: a survey. *Sensors*, 2023, № 23(4), P. 2362.

УДК 004.451

### ОСНОВНЫЕ ХАРАКТЕРИСТИКИ И ВЫБОР ЗАЩИЩЕННЫХ ОПЕРАЦИОННЫХ СИСТЕМ ДЛЯ КРИТИЧЕСКИХ ИНФРАСТРУКТУР

Селлер Анастасия Романовна

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Большевикова пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

e-mail: seller2005@inbox.ru

**Аннотация.** В условиях активной цифровизации и роста киберугроз проблема выбора защищенной операционной системы (далее ЗОС) для государственных и корпоративных информационных систем приобретает критическую важность. В тезисах рассматриваются ключевые аспекты современных ЗОС, проводится анализ их особенностей на примере решений Astra Linux, Альт СП и механизма безопасности SELinux. Основное внимание уделяется их архитектурным особенностям, соответствию требованиям регуляторов, таким как ФСТЭК России, а также применимости в различных сценариях. Определяются сильные и слабые стороны каждой платформы и формулируются рекомендации по их выбору в зависимости от конкретных задач и нормативных ограничений.

**Ключевые слова:** операционные системы; защита информации; государственные информационные системы; корпоративная безопасность; сравнительная оценка; стандарты ФСТЭК; Astra Linux; Альт СП; SELinux.

### MAIN CHARACTERISTICS AND SELECTION OF SECURED OPERATING SYSTEMS FOR CRITICAL INFRASTRUCTURE

Seller Anastasiia

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

22 Bolshhevikov Av, bldg 1, St. Petersburg, 193232, Russia

e-mail: seller2005@inbox.ru

**Abstract.** In the context of active digitalization and the growing number of cyber threats, the issue of choosing a secure operating system (hereinafter referred to as SOS) for government and corporate information systems has become critically important. This article explores the key aspects of modern SOSs and analyzes their features using the examples of Astra Linux, Alt SP, and the SELinux security mechanism. The focus is on their architectural features, compliance with regulatory requirements such as those of the Federal Service for Technical and Export Control of Russia, and their

applicability in various scenarios. The strengths and weaknesses of each platform are identified, and recommendations are made for selecting them based on specific tasks and regulatory constraints.

**Keywords:** operating systems; information protection; state information systems; corporate security; comparative assessment; FSTEC standards; Astra Linux; Alt SP; SELinux.

Актуальность выбора защищенной операционной системы обусловлена необходимостью обеспечения конфиденциальности и целостности данных в условиях возрастающего количества целевых атак и строгих нормативных требований. В фокусе анализа — три решения: Astra Linux, Альт СП и SELinux, широко используемые в РФ и мире.

Ключевые требования к ЗОС. Защищенные ОС должны обеспечивать не только базовый функционал, но и реализовывать встроенные механизмы безопасности. К базовым требованиям относятся: реализация мандатного и дискреционного контроля доступа, изоляция процессов и ресурсов, обеспечение целостности системных компонентов, ведение детального аудита безопасности и наличие официальной сертификации. В России ключевым регулятором выступает ФСТЭК, устанавливающий классы защищенности [1–3]. Для международного применения актуален стандарт Common Criteria (ISO/IEC 15408).

Краткий обзор анализируемых платформ. Astra Linux — отечественная ОС, сертифицированная ФСТЭК и ФСБ для высших классов защищенности. Ключевая особенность — модульная система мандатного и ролевого разграничения доступа, обеспечивающая глубокую изоляцию и контроль целостности. Платформа основана на ядре Linux и ориентирована на госсектор и силовые структуры [4, 5].

Альт СП — защищенный дистрибутив от «Базальт СПО», также сертифицированный по требованиям ФСТЭК. Реализует средства мандатного контроля, встроенный аудит и защиту от НСД. Архитектурно представляет собой монолитное ядро с усиленными механизмами безопасности, предназначен для госучреждений и бизнеса, работающего с конфиденциальной информацией.

SELinux — не самостоятельная ОС, а модуль безопасности для ядра Linux. Реализует гибкую модель мандатного доступа через политики безопасности. Требуется высокой квалификации для настройки и не имеет отечественной сертификации, что ограничивает его применение в госструктурах РФ. Широко используется в корпоративном секторе, банках и дата-центрах за рубежом.

Сравнительные аспекты. Сравнительный анализ позволяет выявить ниши каждой из систем. Отечественные решения (Astra Linux и Альт СП) демонстрируют полное соответствие требованиям российских регуляторов, что делает их предпочтительными для государственных и оборонных заказчиков. Их слабыми сторонами можно считать относительную сложность настройки и среднюю производительность.

SELinux, напротив, показывает высокую гибкость и производительность, идеально интегрируясь в корпоративные и облачные инфраструктуры. Однако отсутствие сертификации ФСТЭК и высокая сложность администрирования являются существенными барьерами для его широкого использования в РФ [6].

Перспективы развития. Эволюция защищенных ОС будет идти по пути интеграции с облачными и виртуализированными средами. Важным трендом станет внедрение технологий искусственного интеллекта и машинного обучения для автоматизации обнаружения угроз и реагирования на инциденты. Также ожидается оптимизация производительности и внедрение более эффективных криптографических алгоритмов для противодействия современным угрозам.

Выбор конкретной ЗОС является стратегической задачей и должен основываться на трех ключевых факторах: нормативные требования (наличие сертификации ФСТЭК), специфика решаемых задач и доступность экспертизы для развертывания и поддержки. Для российских госструктур оптимальны сертифицированные отечественные решения Astra Linux и Альт СП. Для международных корпоративных проектов, где допустимо использование зарубежных решений, SELinux может быть предпочтительнее. Дальнейшее развитие ЗОС будет направлено на повышение их адаптивности и автоматизации.

## СПИСОК ЛИТЕРАТУРЫ

1. Штеренберг, С. И. Методика обеспечения безопасности доменных систем доверенной зоны / С. И. Штеренберг, Г. С. Бударный, И. В. Чумаков // Региональная информатика и информационная безопасность : Сборник трудов Юбилейной XVIII Санкт-Петербургской международной конференции, Санкт-Петербург, 26–28 октября 2022 года. Том Выпуск 11. Санкт-Петербург: Региональная общественная организация «Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления», 2022. С. 621–625. EDN CHZCRU.
2. Штеренберг, С. И. Анализ безопасности доменных систем / С. И. Штеренберг, Г. С. Бударный, И. В. Чумаков // Региональная информатика (РИ-2022) : Юбилейная XVIII Санкт-Петербургская международная конференция. Материалы конференции, Санкт-Петербург, 26–28 октября 2022 года. Санкт-Петербург: Региональная общественная организация «Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления», 2022. С. 587–588. EDN EGVVFU.
3. Исследование концепции ядра в различных операционных системах / Г. С. Бударный, А. А. Казанцев, С. А. Руденко, Д. Н. Смирнов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022) : Сборник научных статей XI Международной научно-технической и научно-методической конференции. В 4-х томах, Санкт-Петербург, 15–16 февраля 2022 года / Под редакцией А.В. Шестакова, сост. В.С. Елагин, Е.А. Аникевич. Том 4. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2022. С. 411–417. EDN QZWOOF.
4. Алехин, Р. В. Статистические методы анализа данных / Р. В. Алехин, Г. С. Бударный, А. О. Камалова // Студенческая весна - 2024 : Сборник научных статей 78-ой региональной научно-технической конференции студентов, аспирантов и молодых ученых, Санкт-Петербург, 15 мая 2024 года. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2024. С. 53–57. EDN HZDTTS.
5. Астра Линукс. Официальный сайт. URL: <https://astralinux.ru>
6. Горбунов А. В., Иванов И. С. Исследование качества обеспечения безопасности в ОС Windows и ОС Linux методом сравнительного анализа // Информационные технологии и безопасность. 2023. № 2. С. 58–65.



УДК 004.056.5

## УГРОЗЫ И УЯЗВИМОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАСПРЕДЕЛЁННЫХ ОБЛАЧНЫХ АРХИТЕКТУРАХ

Сенин Олег Геннадьевич, Яровой Роберт Владимирович

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: kr580vm@mail.ru, Nadzar@yandex.ru

**Аннотация.** В тезисе представлено обобщение ключевых угроз, характерных для распределённых облачных систем, предложены актуальные подходы к обеспечению защиты информации, включая унифицированные стратегии, модель Zero Trust и интеллектуальные системы реагирования.

**Ключевые слова:** информационная безопасность; гибридное облако; многооблачная среда; управление доступом; защита данных; утечка информации; Zero Trust.

## INFORMATION SECURITY THREATS AND VULNERABILITIES IN DISTRIBUTED CLOUD ARCHITECTURES

Senin Oleg, Yarovoy Robert

Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: kr580vm@mail.ru, Nadzar@yandex.ru

**Abstract.** The thesis presents a summary of the key threats typical for distributed cloud systems and proposes relevant approaches to ensuring information security, including unified strategies, the Zero Trust model, and intelligent response systems.

**Keywords:** information security; hybrid cloud; multi-cloud environment; access control; data protection; information leakage; Zero Trust.

Рост цифровых мощностей и необходимость масштабируемости подталкивают организации к использованию гибридных и многооблачных инфраструктур. Совмещение частных и публичных ресурсов позволяет балансировать между безопасностью и экономичностью, однако одновременно с этим обнажает новые векторы уязвимости, порождая комплекс рисков на стыке системного администрирования и защиты данных [1].

Одним из наиболее ощутимых вызовов выступает фрагментированность политик безопасности: каждая платформа предлагает собственный стек инструментов и логик, что затрудняет унификацию подходов к контролю доступа, шифрованию, логированию и мониторингу. Модель Shared Responsibility, декларирующая разделение ответственности между поставщиком и потребителем, зачастую реализуется непоследовательно, провоцируя пробелы в безопасности [2].

Отдельной проблемой становится расширение атакуемой поверхности. Обилие API, интерфейсов удалённого доступа и сервисов межоблачной интеграции создаёт множество потенциальных точек вторжения. Многообразие протоколов, политик и механизмов авторизации увеличивает вероятность человеческой ошибки при настройке либо автоматическом обновлении облачных модулей [3].

Рекомендованные меры противодействия включают разработку универсальной стратегии безопасности с акцентом на централизацию контроля, применение модели Zero Trust для сегментации среды и отказа от доверия по умолчанию, внедрение клиентского шифрования с самостоятельным управлением ключами, а также использование систем уровня SIEM и SOAR для автоматизации реагирования [4].

Современные угрозы всё чаще используют искусственный интеллект и машинное обучение: алгоритмы подбора фишинг-сценариев, генерации deepfake-контента и обхода поведенческих фильтров становятся всё доступнее. В связи с этим необходим переход от реактивной к проактивной модели обеспечения безопасности, включающей DevSecOps как парадигму непрерывного внедрения защиты на всех этапах жизненного цикла сервисов [4].

Таким образом, защита гибридных и многооблачных инфраструктур требует не изолированных решений, а целостной системы с интеллектуальной адаптацией к угрозам и встроенной культурой кибергигиены.

## СПИСОК ЛИТЕРАТУРЫ

1. Солодухин Б. В., Рябов Г. А., Боголепов Г. С., Яровой Р. В. Подход к решению задачи оптимального выбора программных средств защиты информации в автоматизированных системах управления // Национальная безопасность России: актуальные аспекты. Сборник избранных статей Всероссийской научно-практической конференции. СПб, 2021. С. 31-36.
2. Яровой Р. В., Кривоногова Е. В., Рябов Г. А. Атаки на веб-приложения: определение, типы и профилактика // Тенденции развития науки и образования. 2023. № 101-4. С. 96-98.
3. Иванов А. Ю., Саенко И. Б. Анализ возможностей перспективных моделей разграничения доступа к информации в облачных инфраструктурах // Региональная информатика «РИ-2018». Материалы конференции. СПб., 2018. С. 139-141.
4. Бекматов А. К., Кутдусова Э. Р., Мукимов Ш. И., Давлатова Н. Н. Прогрессивные тенденции применения искусственного интеллекта в области информационной безопасности // Экономика и социум. 2023. № 6 (109). С. 1264-1270.

УДК 004.056.5

**УГРОЗЫ И ЗАЩИТА В ИНФРАСТРУКТУРЕ КОНТЕЙНЕРИЗАЦИИ:  
АНАЛИЗ ПОДХОДОВ И ПРАКТИК БЕЗОПАСНОСТИ****Сенин Олег Геннадьевич, Яровой Роберт Владимирович**

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: kr580vm@mail.ru, Nadzar@yandex.ru

**Аннотация.** В тезисе рассмотрены ключевые уязвимости контейнерных систем, описаны подходы к их выявлению и нейтрализации, включая DevSecOps, сканирование образов, политику изоляции и мониторинг активности. Особое внимание уделяется интеграции безопасности в жизненный цикл разработки и эксплуатации.

**Ключевые слова:** контейнеризация; безопасность; Docker; Kubernetes; DevSecOps; контроль доступа.

**THREATS AND SECURITY IN CONTAINERIZATION INFRASTRUCTURE:  
ANALYSIS OF SECURITY APPROACHES AND PRACTICES****Senin Oleg, Yarovoy Robert**

Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: kr580vm@mail.ru, Nadzar@yandex.ru

**Abstract.** The thesis examines key vulnerabilities of container systems, describes approaches to their detection and neutralization, including DevSecOps, image scanning, isolation policy and activity monitoring. Particular attention is paid to the integration of security into the development and operation lifecycle.

**Keywords:** containerization; security; Docker; Kubernetes; DevSecOps; access control.

Переход к контейнеризированной инфраструктуре влечёт за собой не только архитектурные преимущества, но и трансформацию угроз, выходящих за рамки традиционной модели безопасности. Использование общих ядер, автоматизированных CI/CD-процессов и публичных реестров контейнеров порождает новые вариации атак [1].

Наиболее уязвимыми оказываются образы, загружаемые из неконтролируемых источников, которые зачастую содержат устаревшие библиотеки и критические уязвимости, скрытые внутри слоёв. Нарушения принципа минимизации и отсутствие цифровых подписей затрудняют контроль целостности и происхождения компонентов. Побег из контейнера через монтирование чувствительных директорий или запуск с привилегиями представляет реальный риск для всей хостовой системы [2].

Оркестраторы, такие как Kubernetes, хотя и обеспечивают отказоустойчивость, в условиях слабой настройки превращаются в атакуемую точку: открытые API, недостаточная сегментация сети и неправильные RBAC-настройки открывают подвергают систему различным рискам [3].

Использование минималистичных образов и проверка их содержимого с помощью Trivy, Clair или Anchore Engine позволяет предотвратить попадание уязвимого ПО в продуктивную среду. Мониторинг событий ядра средствами Falco и внедрение политик доступа на уровне кластеров обеспечивают базовую защиту [4].

Наивысшую эффективность демонстрирует подход DevSecOps, предполагающий интеграцию проверки безопасности в каждый этап жизненного цикла контейнера. Проверка Dockerfile, автоматическая блокировка образов с уязвимостями, применение подписей (например, Cosign) и автоматизированная валидация политик через OPA формируют непрерывный защитный контур.

Развитие AI-инструментов для обнаружения аномалий, внедрение gVisor и Kata Containers для глубокой изоляции, а также настройка логирования и визуализации (Prometheus, Grafana) становятся обязательными элементами зрелой инфраструктуры.

Таким образом, безопасность контейнеризации — это не набор инструментов, а целостный процесс, предполагающий осознание уязвимостей, своевременное внедрение практик и постоянное отслеживание угроз. Только при сочетании архитектурной строгости и автоматизации можно гарантировать устойчивость к атакам.

**СПИСОК ЛИТЕРАТУРЫ**

1. Баранов М. В., Дубов И. Р. Важность контейнеризации в приложениях с микросервисной архитектурой // Информационные технологии в моделировании и управлении: подходы, методы, решения. Сборник материалов VII Всероссийской научной конференции с международным участием. Тольятти, 2024. С. 200-206.
2. Наумова К. С., Переспелов А. В. Безопасность виртуальной контейнеризации в ИТ-технологиях // Информационные технологии и системы: управление, экономика, транспорт, право. 2020. № 4 (40). С. 22-25.
3. Лытнев Т. Д. Обзор способов предотвращения атак при разработке и эксплуатации контейнеризированных приложений // Научный аспект. 2024. Т. 46. № 6. С. 5820-5829.
4. Солодухин Б. В., Рябов Г. А., Боголепов Г. С., Яровой Р. В. Подход к решению задачи оптимального выбора программных средств защиты информации в автоматизированных системах управления // Национальная безопасность России: актуальные аспекты. Сборник избранных статей Всероссийской научно-практической конференции. СПб., 2021. С. 31-36.

УДК 004.056.5

**LLM КАК ИНСТРУМЕНТ ДЕТЕКТИРОВАНИЯ И ПРОГНОЗИРОВАНИЯ КИБЕРУГРОЗ****Сенин Олег Геннадьевич, Яровой Роберт Владимирович**

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: kr580vm@mail.ru, Nadzar@yandex.ru

**Аннотация.** Тезис освещает возможности LLM в обнаружении фишинга, вредоносных скриптов, атак на цепочки поставок, а также подчеркивает их прогностические и объяснимые свойства. Рассмотрены архитектурные подходы, практики адаптации, сопровождающие интеграцию моделей в защитные системы.

**Ключевые слова:** большие языковые модели; информационная безопасность; искусственный интеллект.

**LLM AS A TOOL FOR DETECTING AND FORECASTING CYBER THREATS****Senin Oleg, Yarovoy Robert**

Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: kr580vm@mail.ru, Nadzar@yandex.ru

**Abstract.** The thesis highlights the capabilities of LLM in detecting phishing, malicious scripts, supply chain attacks, and emphasizes their predictive and explainable properties. Architectural approaches and adaptation practices accompanying the integration of models into security systems are considered.

**Keywords:** large language models; information security; artificial intelligence.

Многоэтапные и замаскированные атаки на информационные системы требуют принципиально новых методов детектирования, выходящих за рамки традиционной сигнатурной аналитики. Большие языковые модели (LLM), опирающиеся на архитектуру трансформеров, становятся ядром этой парадигмальной трансформации [1].

Основные преимущества LLM заключаются в способности к семантическому анализу, выявлению сложных взаимосвязей и адаптации к новым векторам угроз. Применение LLM позволяет анализировать логи, письма, скрипты и техническую документацию как единый смысловой поток, выстраивая целостную картину инцидента, включая его скрытую подготовку [2].

Ключевым аспектом становится способность моделей к интерпретации неструктурированных данных: фишинговые письма анализируются по стилю, контексту и прагматике; вредоносные скрипты — через обфускацию, подозрительные вызовы и синтаксические шаблоны (CodeBERT); аномалии поведения — в формате временных зависимостей между событиями. Такие подходы превосходят классические системы, ограниченные жесткими правилами [3].

Преимущество LLM в упреждающем обнаружении выражается в анализе обсуждений на форумах, утечек и новостей, где модели выявляют зарождающиеся паттерны атак. Это позволяет формировать повестку защиты до момента активного применения эксплойтов. Однако подобные возможности сопровождаются и вызовами: значительное потребление ресурсов, сложность валидации решений и потенциальные риски злоупотреблений при автономной генерации сценариев [4].

Современные LLM способны формулировать выводы в понятной аналитикам форме, что делает возможной гибридную модель — автоматическая диагностика с экспертной интерпретацией. В условиях дефицита квалифицированных специалистов такой подход позволяет повысить эффективность реагирования и снизить человеческий фактор.

Тем не менее, полная интеграция LLM требует решения этических и организационных задач. Вопросы защиты обучающих данных, контроль за автономными действиями модели, а также устойчивость к целенаправленным атакам на саму модель формируют новое поле для регуляции и исследований [5].

Таким образом, использование LLM в кибербезопасности не сводится к расширению инструментария — оно представляет собой переход к интеллектуальной автоматизации анализа угроз, обладающей прогностическим и адаптивным потенциалом.

**СПИСОК ЛИТЕРАТУРЫ**

1. Абраменко Г. Т., Котенко И. В. Анализ и перспективы применения LLM в информационной безопасности // Региональная информатика (РИ-2024). Материалы XIX Санкт-Петербургской международной конференции. СПб., 2024. С. 88-89.
2. Солодухин Б. В., Рябов Г. А., Боголепов Г. С., Яровой Р. В. Подход к решению задачи оптимального выбора программных средств защиты информации в автоматизированных системах управления // Национальная безопасность России: актуальные аспекты. Сборник избранных статей Всероссийской научно-практической конференции. СПб., 2021. С. 31-36.
3. Аверина Ю. А. Влияние искусственного интеллекта на кибербезопасность // Студенческий форум. 2024. № 18-1 (285). С. 34-36.
4. Бекматов А. К., Кутдусова Э. Р., Мукимов Ш. И., Давлатова Н. Н. Прогрессивные тенденции применения искусственного интеллекта в области информационной безопасности // Экономика и социум. 2023. № 6 (109). С. 1264-1270.
5. Шагдуров Б. Б. Этические риски в общении с чат-ботом со встроенным искусственным интеллектом // Аналитические технологии в социальной сфере: теория и практика. 2023. С. 71-79.

УДК 004.056.5

**LLM КАК ИНТЕЛЛЕКТУАЛЬНЫЙ ИНСТРУМЕНТ РЕВЕРС-ИНЖИНИРИНГА  
ВРЕДНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ****Сенин Олег Геннадьевич, Яровой Роберт Владимирович**

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: kr580vm@mail.ru, Nadzar@yandex.ru

**Аннотация.** В тезисе рассмотрены сценарии применения LLM для генерации аннотаций, анализа дизассемблированных функций, идентификации шаблонов поведения и интеграции в автоматизированные цепочки реагирования.

**Ключевые слова:** вредоносное ПО; реверс-инжиниринг; большие языковые модели; LLM; автоматизация анализа кода; кибербезопасность; статический анализ; интерпретация байт-кода.

**LLM AS AN INTELLIGENT TOOL FOR REVERSE ENGINEERING OF MALWARE****Senin Oleg, Yarovoy Robert**

Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: kr580vm@mail.ru, Nadzar@yandex.ru

**Abstract.** The thesis examines scenarios for using LLM to generate Abstracts, analyze disassembled functions, identify behavior patterns, and integrate into automated response chains.

**Keywords:** malware; reverse engineering; large language models; LLM; code analysis automation; cybersecurity; static analysis; bytecode interpretation.

Масштаб и разнообразие современных вредоносных программ требуют перехода от полностью ручного реверс-инжиниринга к гибридным интеллектуальным системам анализа. Большие языковые модели (LLM), способные интерпретировать низкоуровневый код, становятся перспективным инструментом в ускорении и стандартизации анализа вредоносного ПО [1].

Модели нового поколения, обученные на текстах и исходных кодах, демонстрируют способность к восстановлению логики функций, генерации псевдокода, распознаванию шаблонов поведения и предположению назначения блоков кода. Аналитик получает возможность быстро очертить структуру подозрительного файла, выявив механизмы шифрования, инъекции DLL, обхода UAC или кейлоггинга [2].

Интерактивность LLM позволяет использовать их в диалоговом режиме: модель комментирует исполняемый код, предлагает гипотезы, уточняет логику функций на основе ключевых вызовов. Это снижает когнитивную нагрузку и расширяет круг специалистов, способных участвовать в реверс-анализе. Возможно подключение LLM к дизассемблерам (IDA Pro, Ghidra) через API, что обеспечивает автоматическую подстановку аннотаций и оценку подозрительных сегментов [3].

Применение моделей также актуально при анализе обфусцированного кода, где традиционные средства сталкиваются с бессмысленными вставками и запутанными переходами. LLM выявляют антиотладочные приёмы, прогнозируют семантику функций и формируют предположения даже в условиях отсутствия прямых сигнатур.

В массовом режиме LLM могут выполнять классификацию и категоризацию вредоносных образцов, создавать поведенческие досье и автоматически извлекать индикаторы компрометации (IOC), формируя отчёты для служб реагирования и CERT. В связке с YARA-правилами возможна генерация сигнатур и их объяснение в человекопонятной форме [4].

Предлагается методика, включающая сравнение результатов работы LLM с эталонной экспертной разметкой по метрикам точности, полноты и интерпретируемости.

Таким образом, LLM трансформируют задачи реверс-инжиниринга, превращая ручной труд в поддерживаемый процесс с интеллектуальной автоматизацией и снижением барьера входа.

**СПИСОК ЛИТЕРАТУРЫ**

1. Лукашенко В. И., Яровой Р. В. Роль искусственного интеллекта в информационной безопасности // Региональная информатика и информационная безопасность. Сборник трудов Санкт-Петербургской международной конференции и Санкт-Петербургской межрегиональной конференции. СПб., 2024. С. 121-124.
2. Мишин Д. В., Иванов А. П. Обнаружение признаков вредоносного кода с помощью нейросетевых технологий // Труды международного симпозиума «Надежность и качество». 2024. Т. 1. С. 328-333.
3. Намиот Д. Е., Ильюшин Е. А. Искусственный интеллект в кибербезопасности: поиск вредоносного программного обеспечения // International Journal of Open Information Technologies. 2024. Т. 12. № 6. С. 143-149.
4. Яровой Р. В., Рябов Г. А., Карганов В. В. Кибербезопасность в мире инфотелекоммуникаций: вызовы и стратегии защиты // Инновационная деятельность в Вооруженных Силах Российской Федерации. Труды всероссийской научно-практической конференции. СПб., 2023. С. 373-377.

УДК 004.056

**LLM В СЛУЖБЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ПРАКТИЧЕСКИЕ СЦЕНАРИИ, УЯЗВИМОСТИ И ГРАНИЦЫ ПРИМЕНИМОСТИ****Сенин Олег Геннадьевич, Яровой Роберт Владимирович**

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: kr580vm@mail.ru, Nadzar@yandex.ru

**Аннотация.** В тезисе обобщены ключевые сценарии использования больших языковых моделей (LLM) для анализа логов, вредоносного кода, документирования и проверки политик. Освещены преимущества, ограничения, включая риски утечки данных, ошибочных выводов и атак на входной запрос.

**Ключевые слова:** информационная безопасность; большие языковые модели; LLM; реверс-инжиниринг.

**LLM IN INFORMATION SECURITY: PRACTICAL SCENARIOS, VULNERABILITIES AND APPLICABILITY LIMITS****Senin Oleg, Yarovoy Robert**

Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: kr580vm@mail.ru, Nadzar@yandex.ru

**Abstract.** The paper summarizes key use cases of large language models (LLM) for log analysis, malware analysis, documentation, and policy verification. It highlights the benefits, limitations, and risks of data leakage, false positives, and input request attacks.

**Keywords:** information security; large language models; LLM; reverse engineering.

В условиях усложняющегося ландшафта киберугроз и перегрузки специалистов по информационной безопасности большими объемами данных, большие языковые модели становятся инструментами интеллектуальной поддержки. Их универсальность позволяет применять их в задачах интерпретации логов, анализа вредоносного кода, генерации документации и симуляции атак [1].

LLM способны выделять аномалии в логах SIEM-систем, формулировать гипотезы по инцидентам и преобразовывать сложные записи в легко усваиваемые формулировки. При реверс-анализе вредоносного ПО модели объясняют дизассемблированный код, предлагают классификацию функций и даже помогают формировать сигнатуры. В области анализа политик безопасности они применимы для выявления формальных несоответствий, предложений по адаптации и стандартизации внутренней документации [2–3].

На практике модели облегчают принятие решений, ускоряют рутинные процессы и снижают порог входа для начинающих аналитиков. Однако надёжность LLM не является абсолютной. Возможны логически правдоподобные, но ошибочные интерпретации, особенно при недостатке контекста. Наблюдается уязвимость к манипулятивному вводу — prompt injection — способному повлиять на поведение модели [4].

Существенный риск представляет передача конфиденциальной информации в облачные API-модели, особенно при анализе логов, исходного кода или регламентов. Без изоляции среды и ограничения доступа возможно непреднамеренное раскрытие чувствительных данных.

На организационном уровне важна интеграция LLM в процессы инцидент-менеджмента и обучение персонала. Их использование в Центрах оперативного реагирования позволяет автоматизировать обработку поступающих событий, фильтрацию и первоначальную категоризацию, оставляя специалистам задачи интерпретации и принятия решений. При этом необходимо учитывать этическую и юридическую сторону автоматизированной генерации: модель не может подменить ответственность человека [5].

Таким образом, LLM формируют новый класс инструментов в сфере ИБ — не универсальные решения, но интеллектуальные помощники, усиливающие компетенции аналитика при соблюдении правил безопасной интеграции и критического отношения к результатам их работы.

**СПИСОК ЛИТЕРАТУРЫ**

1. Лукашенко В. И., Яровой Р. В. Роль искусственного интеллекта в информационной безопасности // Региональная информатика и информационная безопасность. Сборник трудов Санкт-Петербургской международной конференции и Санкт-Петербургской межрегиональной конференции. Санкт-Петербург, 2024. С. 121-124.
2. Мишин Д. В., Иванов А. П. Обнаружение признаков вредоносного кода с помощью нейросетевых технологий // Труды международного симпозиума «Надежность и качество». 2024. Т. 1. С. 328-333.
3. Намиот Д. Е., Ильюшин Е. А. Искусственный интеллект в кибербезопасности: поиск вредоносного программного обеспечения // International Journal of Open Information Technologies. 2024. Т. 12. № 6. С. 143-149.
4. Конев А. А., Паюсова Т. И. Большие языковые модели в информационной безопасности и тестировании на проникновение: систематический обзор возможностей применения // Научно-технический вестник информационных технологий, механики и оптики. 2025. Т. 25. № 1. С. 42-52.
5. Резников Р. М. Искусственный интеллект в информационной безопасности // Автоматизация в промышленности. 2025. № 2. С. 33-42.

УДК 004.056

**ОБНАРУЖЕНИЕ УЯЗВИМОСТЕЙ В ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ  
НА ОСНОВЕ ОБУЧЕНИЯ С ПОДКРЕПЛЕНИЕМ****Слётков Максим Алексеевич<sup>1</sup>, Котенко Игорь Витальевич<sup>2</sup>**<sup>1</sup> Университет ИТМО

Кронверкский пр., 49, Санкт-Петербург, 197101, Россия

<sup>2</sup> СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия

e-mails: sletovo@gmail.com, ivkote@comsec.spb.ru

**Аннотация.** Современные средства автоматизированного тестирования на проникновение обладают рядом ограничений, существенно снижающих эффективность их применения при анализе защищённости информационных систем. Наиболее распространённые инструменты демонстрируют низкую гибкость в адаптации к различным архитектурам целевых систем, что ограничивает полноту моделирования потенциальных угроз. В работе рассматривается подход, основанный на использовании обучения с подкреплением для имитации поведения атакующих в реальной среде. Такой подход позволяет приблизить процесс автоматического пентеста к условиям реальных атак, повышая степень вариативности и реалистичности сценариев проникновения.

**Ключевые слова:** информационная безопасность; пентест; обучение с подкреплением; сетевая безопасность; машинное обучение.

**DETECTION OF VULNERABILITIES IN INFORMATION AND COMPUTING NETWORKS  
BASED ON REINFORCED LEARNING****Maksim Sletov<sup>1</sup>, Kotenko Igor<sup>2</sup>**<sup>1</sup> The St. Petersburg National Research University of Information Technologies, Mechanics and Optics

49 Kronverksky Av, St. Petersburg, 197101, Russia

<sup>2</sup> St. Petersburg Federal Research Center of the Russian Academy of Sciences

39 14th Line VO, St. Petersburg, 199178, Russia

e-mails: sletovo@gmail.com, ivkote@comsec.spb.ru

**Abstract.** Modern automated penetration testing tools have a number of limitations that significantly reduce their effectiveness when analyzing the security of information systems. The most common tools demonstrate low flexibility in adapting to different target system architectures, which limits the completeness of potential threat modeling. The paper discusses an approach based on the use of reinforcement learning to simulate attacker behavior in a dynamic environment. This approach allows the automatic penetration testing process to be brought closer to real-world attack conditions, increasing the variability and realism of penetration scenarios.

**Keywords:** information security; penetration testing; reinforcement learning; network security; machine learning.

Тестирование систем на проникновение с целью выявления уязвимостей и слабых мест в защите остаётся одной из приоритетных задач в сфере информационной безопасности [1–4]. Особое значение эта проблема приобретает для информационно-вычислительных сетей, где компрометация инфраструктуры может привести к серьёзным последствиям [5–8]. Автоматизированное тестирование на проникновение позволяет оценивать степень защищённости инфраструктуры и выявлять потенциальные угрозы без необходимости непосредственного участия человека на каждом этапе процесса. В условиях минимальной информации о целевой системе особое значение приобретают методы, способные адаптироваться к неопределённости среды и самостоятельно вырабатывать оптимальные стратегии поиска уязвимостей [9]. Одним из перспективных направлений в этой области является применение обучения с подкреплением, которое позволяет агентам накапливать и использовать опыт взаимодействия с моделью среды для оптимизации своих действий [10, 11].

Несмотря на перспективность применения обучения с подкреплением для автоматического пентеста, данный подход сталкивается с рядом значимых проблем. Одной из ключевых трудностей является высокая длительность процесса обучения, обусловленная необходимостью многократного взаимодействия агента с моделью среды для накопления достаточного опыта. По мере усложнения инфраструктуры увеличивается и время, необходимое для формирования эффективной политики. Это может приводить к задержкам в внедрении готовых решений и увеличению периода уязвимости защищаемых систем [12].

Одним из наиболее перспективных подходов к сокращению времени обучения в задачах автоматизированного пентеста является масштабирование процесса за счёт увеличения числа обучаемых агентов [5]. Такая организация позволяет одновременно исследовать несколько сценариев, ускоряя накопление опыта и снижая вероятность достижения локальных максимумов функции вознаграждения [13–15].

В рамках представленного исследования был рассмотрен подход, основанный на параллельном обучении нескольких агентов в независимых виртуальных средах. Благодаря этому достигается разнообразие получаемого опыта, что способствует ускоренному формированию оптимальных политик, так как результаты действий одного агента дополняют знания, накопленные другими, сокращая общее время обучения. Такой подход демонстрирует высокую перспективность для автоматизированного тестирования на проникновение в информационно-

вычислительных и промышленных сетях, обеспечивая более быструю сходимость алгоритмов и более полное моделирование атакующих действий при меньшем участии человека.

*Исследование выполнено за счет гранта Российского научного фонда № 25-11-20028, <https://rscf.ru/project/25-11-20028/>.*

#### СПИСОК ЛИТЕРАТУРЫ

1. Kotenko I., Stepashkin M. Analyzing Vulnerabilities and Measuring Security Level at Design and Exploitation Stages of Computer Network Life Cycle // Lecture Notes in Computer Science. 2005. Т. 3685. LNCS. P.311-324.
2. Kotenko I., Stepashkin M. Network Security Evaluation based on Simulation of Malefactor's Behavior // Proceedings. International Conference on Security and Cryptography, SECRIPT 2006. Polytechnic Institute of Setubal. Setubal, 2006. P.339-344.
3. Kotenko I., Chechulin A., Novikova E. Attack Modelling and Security Evaluation for Security Information and Event Management // SECRIPT 2012. International Conference on Security and Cryptography // Proceedings. Rome, Italy. 24-27 July 2012. —P.391-394. ISBN 978-989-8565-24-2.
4. Kotenko I., Chechulin A. Computer attack modeling and security evaluation based on attack graphs // Proceedings of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems. IDAACS 2013. 2013. 2. P. 614-619.
5. Tran K. et al. Deep hierarchical reinforcement agents for automated penetration testing // arXiv preprint arXiv:2109.06449. 2021.
6. Zhou S. et al. Autonomous penetration testing based on improved deep q-network // Applied Sciences. 2021. Т. 11, № 19. P. 8823.
7. Chowdhary A. et al. Autonomous security analysis and penetration testing // 2020 16th International Conference on Mobility, Sensing and Networking (MSN). IEEE, 2020. P. 508-515.
8. Десницкий В.А., Чечулин А.А., Котенко И.В., Левшун Д.С., Коломеец М.В. Комбинированная методика проектирования защищенных встроенных устройств на примере системы охраны периметра // Труды СПИИРАН. 2016. № 5 (48). С. 5-31.
9. Branitskiy A., Kotenko I. Hybridization of computational intelligence methods for attack detection in computer networks // Journal of Computational Science. 2017. Vol.23. P.145-156.
10. Hu Z., Beuran R., Tan Y. Automated penetration testing using deep reinforcement learning // 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE, 2020. P.2-10.
11. AlMajali A. et al. Automated vulnerability exploitation using deep reinforcement learning // Applied Sciences. 2024. Т. 14. №. 20. С. 9331.
12. Wong A. et al. Deep multiagent reinforcement learning: Challenges and directions // Artificial Intelligence Review. 2023. Т. 56. №. 6. С. 5023-5056.
13. Chen J. et al. GAIL-PT: An intelligent penetration testing framework with generative adversarial imitation learning // Computers & Security. 2023. Vol.126. P.103055.
14. Standen M. et al. Cyborg: A gym for the development of autonomous cyber agents // arXiv preprint arXiv:2108.09118. 2021.
15. Li L., Fayad R., Taylor A. Cygil: A cyber gym for training autonomous agents over emulated network systems // arXiv preprint arXiv:2109.03331. 2021.

УДК 004.056

#### ОБНАРУЖЕНИЕ АТАК НА ВЕБ-ПРИЛОЖЕНИЯ С ИСПОЛЬЗОВАНИЕМ КОМБИНИРОВАННОГО ПОДХОДА НА ОСНОВЕ MLP

Соболев Павел Сергеевич<sup>1</sup>, Котенко Игорь Витальевич<sup>2</sup>

<sup>1</sup> Университет ИТМО

Кронверкский пр., 49, Санкт-Петербург, 197101, Россия

<sup>2</sup> СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия

e-mails: 242569@niuitmo.ru, ivkote@comsec.spb.ru

**Аннотация.** В работе предложен комбинированный подход к обнаружению атак на веб-приложения. Проведено тестирование на нескольких наборах данных с различными гибридными моделями на основе многослойного парсептрона. Предложенный подход позволяет повысить точность обнаружения атак на веб-приложения, а также снизить время принятия решения для работы в реальных системах.

**Ключевые слова:** информационная безопасность; безопасность веб-приложений; атаки на веб-приложения; глубокое обучение; машинное обучение.

#### DETECTING ATTACKS ON WEB APPLICATIONS USING A COMBINED MLP-BASED APPROACH

Sobolev Pavel<sup>1</sup>, Kotenko Igor<sup>2</sup>

<sup>1</sup> University ITMO

49 Kronverksky Av, St. Petersburg, 197101, Russia

<sup>2</sup> St. Petersburg Federal Research Center of the Russian Academy of Sciences

39 14th Line VO, St. Petersburg, 199178, Russia

e-mails: 242569@niuitmo.ru, ivkote@comsec.spb.ru

**Abstract.** The paper proposes a combined approach to detecting attacks on web applications. Testing was carried out on several datasets with different hybrid models based on a multilayer parseptron. The proposed approach makes it possible to increase the accuracy of detecting attacks on web applications, as well as reduce the decision-making time for working in real systems.

**Keywords:** cybersecurity; web application protection; attacks on web applications; deep learning; machine learning.

Существует множество видов атак на компьютерные сети и приложения [1]. В своем исследовании 2024 года специалисты Bi.Zone web applications firewall (WAF) показали, что ежемесячно по всему миру обнаруживается около тысячи новых уязвимостей в веб-приложениях. Наиболее распространенными из них являются XSS-атаки и SQL-инъекции. В общей сложности на их долю приходится 48% всех видов атак [2].

Выбор в пользу многослойного персептрона (MLP) в качестве базового элемента гибридной модели среди других моделей [3, 4], как традиционных, так и глубокого обучения, обусловлен как практическими результатами предыдущих экспериментов, так и особенностями задач обнаружения атак на веб-приложения. Ранее была исследована архитектура CNN + MLP [5], продемонстрировавшая высокую точность при обнаружении SQL-инъекций и XSS-атак. Однако её эффективность снижалась при работе с набором данных, содержащем множественные типы атак, что частично объяснялось ограниченностью используемой входной информации (анализ только URL-строки).

В рамках настоящей работы в качестве основы выбрана архитектура на базе MLP, поскольку она обеспечивает низкое время отклика и малую вычислительную нагрузку, оставаясь при этом достаточно чувствительной к признакам атак. Это особенно важно при интеграции модели в реальные системы, работающие в условиях ограниченных ресурсов и требующих принятия решений в режиме, близком к реальному времени. В связи с этим были исследованы различные гибридные решения, основанные на MLP, с различными видами предобработки данных, а также проанализированы дополнительные параметры HTTP-запросов для включения их в процесс обучения и классификации. Помимо этого, были рассмотрены дополнительные параметры оценки работоспособности модели - нагрузка на CPU и время классификации. Предложенный комбинированный подход позволяет эффективно обнаруживать атаки на веб-приложения с высокой точностью и низким временем отклика. Использование комбинированного подхода позволяет выявлять различные виды атак, включая и zero-day. В дальнейшем возможно внедрение предложенного метода в системы WAF и решения для мониторинга сетевой безопасности.

*Работа выполнена при частичной финансовой поддержке бюджетной темы FFZF-2025-0016.*

#### СПИСОК ЛИТЕРАТУРЫ

1. Kotenko I. Active vulnerability assessment of computer networks by simulation of complex remote attacks // Proc. 2003 International Conference on Computer Networks and Mobile Computing (ISSNMC 2003), 2003, pP. 40–47, 1243025.
2. Bi.Zone, “Cybercriminals get 2-3 ready-made solutions to attack websites every week,” Online edition «CNews», [Online]. Available: [https://safe.cnews.ru/news/line/2024-11-13\\_bizone\\_kiberprestupniki\\_ezhenedelno](https://safe.cnews.ru/news/line/2024-11-13_bizone_kiberprestupniki_ezhenedelno).
3. Branitskiy A., Kotenko I. Hybridization of computational intelligence methods for attack detection in computer networks // Journal of Computational Science. 2017. Vol.23. P. 145-156.
4. Komashinskiy D., Kotenko I. Malware detection by data mining techniques based on positionally dependent features // Proceedings of the 18th Euromicro Conference on Parallel, Distributed and Network-Based Processing, PDP 2010. Pisa, 2010. P. 617-623.
5. Котенко И.В., Соболев П.С. Обнаружение атак на веб-приложения на основе комбинирования сверточных нейронных сетей и многослойных персептронов // Информатизация и связь 2025. № 2. С. 90-96.

УДК 004.056

#### ЭВОЛЮЦИЯ ФИШИНГА: ОТ МАССОВЫХ РАССЫЛОК К АВТОНОМНЫМ ИИ-АГЕНТАМ

**Стахов Максим Дмитриевич**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mail: mrmixer1234@yandex.ru

**Аннотация.** В статье рассматривается эволюция фишинговых атак как одной из наиболее распространенных и критических киберугроз. Показан технологический прогресс методов фишинга: от примитивных массовых рассылок 1990-х годов до современных сложных кампаний с использованием искусственного интеллекта и автономных LLM-агентов. Проведен анализ ключевых этапов развития фишинга, включая внедрение ботнетов, фарминга, клонирования сайтов, использование zero-day уязвимостей и AI-генеративных технологий. Особое внимание уделено современным тенденциям: применению jailbroken-LLM (таких как WormGPT), монетизации фишинга через подписочные модели и появлению автономных агентов, способных к стратегическому планированию атак. Предложены направления защиты, включающие продвинутый анализ запросов, многофакторную аутентификацию, контроль доступа и участие человека в принятии решений.

**Ключевые слова:** фишинг; эволюция угроз; искусственный интеллект; генеративный ИИ; LLM-агенты; jailbreaking; кибербезопасность; социальная инженерия.

#### THE EVOLUTION OF PHISHING: FROM MASS MAILINGS TO AUTONOMOUS AI AGENTS

**Stakhov Maxim**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications  
22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mail: mrmixer1234@yandex.ru

**Abstract.** The article examines the evolution of phishing attacks as one of the most common and critical cyber threats. It demonstrates the technological progression of phishing methods: from primitive mass mailings of the 1990s to modern complex campaigns using artificial intelligence and autonomous LLM agents. The analysis covers key stages of phishing development, including the introduction of botnets, pharming, site cloning, the use of zero-day vulnerabilities, and AI-generative technologies. Special attention is paid to modern trends: the use of jailbroken LLMs (such as WormGPT), the monetization of phishing through subscription models, and the emergence of autonomous agents capable



of strategic attack planning. Protection directions are proposed, including advanced prompt monitoring, multi-factor authentication, access control, and human-in-the-loop decision making.

**Keywords:** phishing; threat evolution; artificial intelligence; generative AI; LLM agents; jailbreaking; cybersecurity; social engineering.

Фишинговые атаки остаются одной из наиболее распространенных и критических киберугроз на протяжении последних двух десятилетий. Их жертвами становятся все: от обычных интернет-пользователей, до крупных корпораций по всему миру. UK Cyber Security Breaches Survey 2024, 84 % бизнеса и 83 % благотворительных организаций. Атаки типа BEC (Business Email Compromise) остаются одной из самых дорогих угроз с высоким уровнем реализации социальной инженерии [1].

Фишинг — кибератаки с применением социальной инженерии. Их цель — обмануть жертву и получить конфиденциальную информацию. Например, злоумышленники крадут логины и пароли, платёжные данные или доступ к корпоративным системам. Современные атаки применяют комплексные методы: психологические манипуляции и программные инновации. Атаки эволюционировали от массовых спам-рассылок до целевых атак с использованием генеративного искусственного интеллекта. Эволюция фишинга показывает, как менялись атаки.

История фишинга является постоянной адаптацией злоумышленников к меняющимся условиям и развивающимся системам защиты.

1990-е: Эра SMTP-спама и поддельных HTML-форм. Первые фишинговые атаки середины 1990-х основывались на массовой рассылке электронных писем через открытые SMTP-серверы. Сообщения содержали общие текстовые формулировки со ссылкой, ведущей на статическую HTML-страницу. Страница представляла собой имитацию интерфейса сервиса с формой для ввода логина и пароля. Данные из формы отправлялись на примитивный CGI-скрипт, который записывал их в текстовый файл на сервере злоумышленника. Ключевой технологией была сама социальная инженерия, а не сложность кода.

2003: Внедрение ботнетов и инструментов автоматизации. С ростом количества интернет-пользователей злоумышленники столкнулись с проблемой организации атак на такое число людей. Решением проблемы стало создание сетей зомбированных компьютеров (ботнетов), как Bagle или Storm Worm. Технология позволила перейти от ручных рассылок к автоматизированной массовой рассылке миллионов писем в сутки. Внедрение ботнетов позволило профессиональным киберпреступным группировкам выйти на качественно новый уровень, оставив любителей позади.

В то же время появились первые фишинг-киты (phishing kits) – продаваемое в сети ПО, включающее в себя набор скриптов и HTML-страниц, которые даже киберпреступники с малым опытом могли развернуть на веб-хостинге для быстрой атаки.

2005: Фарминг и эксплуатация уязвимостей браузера. Сталкиваясь с тем, что пользователи все чаще распознают поддельные ссылки, злоумышленники разработали и внедрили более сложную технологию — фарминг. Вместо того чтобы завлечь жертву на фальшивый сайт, они перенаправляли ее с легитимного сайта на скомпрометированный. Это достигалось двумя новыми способами: компрометация локальных DNS-серверов для неправильного разрешения доменных имен и эксплуатация уязвимостей браузера, например, модификация файла «hosts» или перенаправления трафика через JavaScript [2].

2011: Zero-day эксплойты и таргетированные атаки. Технологический прорыв произошел с внедрением в фишинг вредоносных вложений. Письма теперь содержали не только ссылки, но и файлы (PDF, Word, Excel), которые использовали «zero-day» уязвимости программного обеспечения. Например, атака на «RSA Security» в 2011 году использовала файл Excel с эксплойтом уязвимости «Adobe Flash». Для этого фишеры начали покупать эксплойты на черном рынке, либо нанимать высококвалифицированных разработчиков. Это ознаменовало переход от массового спама к целевому фишингу.

2015: Клонирование сайтов и обход 2FA. С внедрением двухфакторной аутентификации фишерам потребовались новые технологии для ее обхода. Появились сложные инструменты для клонирования сайтов в реальном времени, такие как Evilginx или Modlishka. Эти инструменты используют продвинутые методы для динамического создания копии целевого веб-сайта. Они анализируют HTML-код, CSS-стили, JavaScript и другие ресурсы оригинального сайта и воссоздают их на подконтрольном злоумышленникам сервере. Эти инструменты работают как прокси-серверы, расположенные между пользователем и настоящим веб-сайтом [3]. Когда жертва пытается войти в систему, ее браузер подключается к поддельному сайту, созданному злоумышленниками. Все данные, которые пользователь вводит (логин, пароль, коды 2FA), перехватываются прокси-сервером и сохраняются. При этом прокси-сервер ретранслирует запросы жертвы на настоящий сайт, чтобы обеспечить видимость нормальной работы сервиса. Это позволило злоумышленникам получать полный доступ к учетным записям жертв, даже несмотря на наличие второго фактора, что стало значительным технологическим прорывом.

2020: AI-генеративный фишинг и атаки на цепочки поставок SaaS. Современная эра фишинга характеризуется использованием искусственного интеллекта (AI) и автоматизации на основе API. Применение генеративных языковых моделей позволяет автоматизировать генерацию фишинговых сообщений, оптимизированных для обхода лингвистических фильтров. Они обеспечивают создание сообщений с высокой степенью грамматической и стилистической корректности на различных языках, что снижает вероятность обнаружения аномалий и облегчает проведение трансграничных атак. AI-голосовые клоны (Vishing) используются в BEC-атаках для имитации голоса в телефонных звонках [4].

Также злоумышленники стали эксплуатировать в своих атаках API SaaS-платформ. Вместо того, чтобы атаковать пользователей напрямую, они компрометируют API-ключи, используемые для доступа к сервисам отправки электронных писем, предоставляемым Software-as-a-Service (SaaS) решениями (Mailchimp, SendGrid) [5]. Это позволяет им напрямую проводить фишинговые атаки, используя ресурсы доверенных и легитимных платформ, что значительно снижает эффективность традиционных почтовых фильтров.

2023: Jailbroken LLM и монетизация фишинга. Наиболее значительный технологический скачок произошел, когда киберпреступники начали активно использовать большие языковые модели (LLM), взламывая их системы безопасности (jailbreaking). WormGPT, основанный на общедоступной модели GPT-J, стал первым коммерческим AI для киберпреступлений. К 2025 году jailbroken-LLM эволюционировали от единичного продукта к многокомпонентным решениям, включающим в себя сервисы поддержки, обновления и дополнительные модули, доступные через Telegram-бота по подписке [5]. Эти jailbroken-LLM способны генерировать убедительные фишинговые письма на нескольких языках, создавать сложные скрипты для кражи учетных данных (например, на PowerShell), разворачивать вредоносный код и даже давать пошаговые инструкции по проведению атаки.

LLM могут создавать фишинговые сообщения, практически неотличимые от человеческих: они грамматически корректны, стилистически достоверны и хорошо адаптированы под конкретную аудиторию, что значительно повышает эффективность фишинговых атак. Эти модели способны генерировать клоны сайтов, автоматизировать phishing kits и создавать код, который облегчает развёртывание фишинговых ресурсов [3].

Из этого развивается концепция автономных LLM-агентов, способных самостоятельно планировать и выполнять фишинг-кампании. Эти агенты демонстрируют стратегическое поведение — они способны скрывать истинные цели атаки, проявлять свойства самосохранения, модифицироваться и адаптироваться, а также маскировать свои действия под легитимное поведение. Также описаны случаи внедрённых «спящих агентов» (sleeping agents), которые остаются незаметными после обучения и активируются позже, обходя механизмы защиты. Поведение автономных LLM-агентов может включать элементы дезинформации, расчёт на игнорирование или саботаж систем безопасности, использование рассуждений (Chain of Thought), которые намеренно ведут к ложным или опасным выводам [3].

В дополнение к рассмотренным угрозам, всё это требует многослойных стратегий защиты. К ним относятся: продвинутый анализ запросов (prompt monitoring), фильтрация вводимых и выводимых данных, проверка происхождения и данных обучения (data lineage), жесткий контроль доступа и участие человека в цикле принятия решений (human-in-the-loop). Также важны архитектурные ограничения, граничные лимиты на ресурсы и глубина сессий, отслеживание поведения моделей, а также разработка средств для выявления автономного, стратегически ориентированного поведения.

С учётом возрастающих рисков фишинга, важно усиливать проекты по безопасности LLM, создавать прозрачные системы проверки, а также развивать исследования методов обнаружения и нейтрализации как автономных, так и замаскированных фишинг-агентов. Только комплексный подход, охватывающий технические, архитектурные и организационные меры, способен противостоять эволюции фишинга в эпоху масштабных языковых моделей.

#### СПИСОК ЛИТЕРАТУРЫ

1. Osamor J., Ashawa M., Shahrabi M., Philip A. The Evolution of Phishing and Future Directions: A Review. [Электронный ресурс] URL: [https://www.researchgate.net/publication/390162988\\_The\\_Evolution\\_of\\_Phishing\\_and\\_Future\\_Directions\\_A\\_Review](https://www.researchgate.net/publication/390162988_The_Evolution_of_Phishing_and_Future_Directions_A_Review) (дата обращения: 20.08.2025).
2. Yu X., Chen X., Xu F. Recovering and Protecting against DNS Cache Poisoning Attacks. [Электронный ресурс] URL: [https://www.researchgate.net/publication/232620743\\_Recovering\\_and\\_Protecting\\_against\\_DNS\\_Cache\\_Poisoning\\_Attacks](https://www.researchgate.net/publication/232620743_Recovering_and_Protecting_against_DNS_Cache_Poisoning_Attacks) (дата обращения: 20.08.2025).
3. Su Y., Zhu S., Zhao Y., Sun P. Let Your Camera See for You: A Novel Two-Factor Authentication Method against Real-Time Phishing Attacks [Электронный ресурс] URL: <https://arxiv.org/abs/2109.00132> (дата обращения: 20.08.2025).
4. Polra V. F. Decoding the Threat Landscape: ChatGPT, FraudGPT, and WormGPT in Social Engineering Attacks. [Электронный ресурс] URL: <https://arxiv.org/abs/2310.05595> (дата обращения: 20.08.2025).
5. Miles Q., Benjamin C. M. Security Concerns for Large Language Models: A Survey. [Электронный ресурс] URL: <https://arxiv.org/abs/2505.18889> (дата обращения: 20.08.2025).

УДК 004.056.5

#### МЕТОДЫ ШИФРОВАНИЯ С ОБЪЕДИНЕНИЕМ ПРОМЕЖУТОЧНЫХ ТЕКСТОВ ПУТЕМ РЕШЕНИЯ СИСТЕМ ЛИНЕЙНЫХ УРАВНЕНИЙ В СХЕМАХ ПСЕВДОВЕРОЯТНОСТНОГО ШИФРОВАНИЯ

Татчина Яна Александровна

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)  
Профессора Попова ул., 5, Санкт-Петербург, 197022, Россия  
e-mail: mondikovay@gmail.com

**Аннотация.** Рассматриваются алгоритмы псевдоловероятностного шифрования, которые позволяют обеспечить размер криптограммы равный сумме размеров двух одновременно шифруемых текстов.

**Ключевые слова:** блочное шифрование; атака с принуждением; псевдоловероятностное шифрование.

## ENCRYPTION METHODS WITH INTERMEDIATE CIPHERTEXT COMBINATION VIA SOLVING SYSTEMS OF LINEAR EQUATIONS IN DENIABLE ENCRYPTION

Tatchina Iana<sup>1</sup>

St. Petersburg State Electrotechnical University «LETI»

5 Professor Popov St, St. Petersburg, 197022, Russia

e-mail: mondikovay@gmail.com

**Abstract.** The paper discusses pseudo-probabilistic encryption algorithms that make it possible to ensure that the size of the ciphertext is equal to the sum of the sizes of two simultaneously encrypted messages.

**Keywords:** block encryption; coercive attack; deniable encryption.

Псевдовероятностное (отрицаемое) шифрование — это криптографический метод, обеспечивающий секретность сообщений, при котором отправитель может после передачи зашифрованного сообщения раскрыть его содержимое и ключ шифрования, если окажется под давлением со стороны злоумышленника, способного оказывать прямое влияние на отправителя и/или получателя. Предполагается, что все сообщения, переданные в ходе сеанса связи, могли быть перехвачены. Схемы отрицаемого шифрования реализованы таким образом, что при необходимости отправитель или получатель могут раскрыть не настоящие, а подставные (фиктивные) данные. При этом протокол отрицаемого шифрования устроен так, чтобы не возникало подозрений, что в зашифрованном тексте может содержаться какое-либо иное сообщение, отличное от предъявленного фиктивного. В случае симметричного шифрования участники используют два ключа: один — секретный, другой — фиктивный, и при принуждении раскрывают только фиктивный ключ. В асимметричных схемах, когда отправитель шифрует сообщение на открытом ключе получателя, возможность имитации достигается тем, что обе стороны в процессе протокола отрицаемого шифрования обмениваются одноразовыми открытыми ключами, которые затем используются для согласования одноразового секретного ключа, применяемого для сокрытия настоящего сообщения [1-3].

Существуют основные требования к алгоритмам отрицаемого шифрования [4]:

- процедуры декодирования при использовании различных ключей должны быть идентичны;
- идентичность использования битов шифртекста для всех возможных значений ключа расшифровывания;
- криптограмма отрицаемого шифрования должна быть неотличима от криптограммы, получаемой методом вероятностного шифрования.

Также важным является возможность сделать размер криптограммы равным сумме размеров двух одновременно шифруемых сообщений. Основная идея таких методов заключается в предварительном шифровании блоков исходных сообщений (что даёт промежуточные шифртексты) и последующем объединении пар соответствующих блоков этих промежуточных шифртекстов в один блок криптограммы. При этом каждый бит итогового блока зависит от всех битов объединяемых промежуточных шифртекстов. В качестве способа объединения используются системы линейных сравнений, где модули выступают в роли элементов секретного ключа. Единый блок криптограммы формируется как решение такой системы сравнений [5].

Наиболее ресурсоемкой операцией в этом процессе является деление на произведение модулей, используемых в системе. Эту концепцию можно применить и в алгоритмах отрицаемого шифрования, если использовать другой способ объединения блоков — решение системы линейных уравнений над конечным полем. В такой системе коэффициенты определяются ключевыми элементами. Обратное значение главного определителя системы можно вычислить заранее, так как оно не меняется при неизменном ключе шифрования. Благодаря этому, при каждом решении системы уравнений в процессе отрицаемого шифрования не потребуется выполнять операцию обращения в конечном поле — достаточно лишь нескольких операций умножения и сложения по модулю простого числа или неприводимого двоичного многочлена (в зависимости от выбранного поля). Поскольку модуль не является секретным, можно вычислять его специальным образом, чтобы ускорить модульное умножение, избавившись от необходимости деления.

Например, при одновременном шифровании двух сообщений решаются системы из двух уравнений, и для каждой из них требуется выполнить всего 6 умножений и 2 сложения (или вычитания). Благодаря отсутствию необходимости многократного обращения в конечном поле, объединение блоков промежуточных шифртекстов на основе решения систем линейных уравнений оказывается значительно менее трудоемким по сравнению с объединением на основе систем сравнений. Это позволяет существенно повысить производительность отрицаемого шифрования.

### СПИСОК ЛИТЕРАТУРЫ

1. Moldovyan A.A., Moldovyan N.A. Practical Method for Bi-Deniable Public-Key Encryption // Quasigroups and related systems. 2014. Vol. 22. Pp. 277-282.
2. Moldovyan N.A., Berezin A.N., Kornienko A.A., Moldovyan A.A., Bi-deniable Public-Encryption Protocols Based on Standard PKI // Proceedings of the 18th FRUCT & ISPIT Conference, 18-22 April 2016, Technopark of ITMO University, Saint-Petersburg, Russia. FRUCT Oy, Finland. Pp. 212-219.
3. Березин А.Н., Биричевский А.Р., Мондикова Я.А. Отрицаемое шифрование для защиты информации от НСД // 5-я научно-практическая конференция «Информационная безопасность. Невский диалог». Санкт-Петербург, 12-13 ноября 2013 г. / СПб.: «Студия «НП-Принт». С. 21-22.
4. Морозова Е.В., Мондикова Я.А., Молдовян Н. А. Способы отрицаемого шифрования с разделяемым ключом // Информационно-управляющие системы. № 6. 2013. С. 73-78.
5. Молдовян, А. А. Способы псевдовероятностного блочного шифрования / А. А. Молдовян, Я. А. Татчина // Интеллектуальные технологии на транспорте. 2018. № 1(13). С. 25-31. EDN YHIGEN.

УДК 004.056.53

**ПОДХОДЫ К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ КРОССЧЕЙН-ВЗАИМОДЕЙСТВИЯ****Теровец Алексей Алексеевич, Кушнир Дмитрий Викторович**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевикова пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mails: a3772636@gmail.com, dima\_kdv@mail.ru

**Аннотация.** В тезисах рассматриваются различные архитектурные подходы и криптографические модели, применяемые для обеспечения безопасности кроссчейн-взаимодействия в современных блокчейн-сетях. Описаны ключевые типы мостов и соответствующие им модели валидации межсетевых событий. Особое внимание уделено типовым уязвимостям, а также анализу компромиссов между безопасностью, децентрализацией, скоростью и экономической эффективностью. Подчёркнута роль zk-доказательств, мультиподписей, оракульных сетей и легких клиентов в обеспечении надёжности и масштабируемости кроссчейн-коммуникации.

**Ключевые слова:** блокчейн; кроссчейн-мост; безопасность блокчейна; мультиподпись; zk-доказательства; легкий клиент; оракул; смарт-контракт; децентрализация; криптография; уязвимость.

**APPROACHES TO ENSURING THE SECURITY OF CROSS-CHAIN INTERACTIONS****Terovec Aleksei, Kushnir Dmitry**

St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruevich  
22 Bolshhevikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mails: a3772636@gmail.com, dima\_kdv@mail.ru

**Abstract.** This paper explores various architectural approaches and cryptographic models used to ensure the security of cross-chain interactions in modern blockchain networks. It outlines the key types of bridges and their corresponding models of interchain event validation. Particular attention is paid to common vulnerabilities, as well as to analyzing trade-offs between security, decentralization, transaction speed, and cost efficiency. The role of zk-proofs, multisignatures, oracle networks, and light clients is emphasized as essential in ensuring the reliability and scalability of cross-chain communication.

**Keywords:** blockchain; cross-chain bridge; blockchain security; multisignature; zk-proofs; light client; oracle; smart contract; decentralization; cryptography; vulnerability.

Современные блокчейн-системы все чаще сталкиваются с задачей эффективного и безопасного взаимодействия между разными сетями, поскольку количество децентрализованных приложений, объемы ликвидности и разнообразие цепей постоянно увеличиваются [1, 2]. В условиях усиливающейся фрагментации экосистемы особую значимость приобретают технологии кроссчейн-коммуникации, которые формируют основу для построения единого цифрового пространства. Ключевым элементом в этом процессе выступают кроссчейн-мосты, однако именно они демонстрируют наибольшую уязвимость: по данным аналитиков, до 70% убытков в секторе децентрализованных финансов за последние годы напрямую связаны с их взломами и ошибками в реализации [3]. С каждым годом такие мосты концентрируют всё больше ликвидности и становятся точкой притяжения для атак, что подчеркивает необходимость всестороннего анализа их безопасности.

Рассмотрим различные типы архитектур кроссчейн-мостов, их ключевые преимущества и ограничения, а также модели обеспечения безопасности и наиболее распространенные уязвимости. Мосты могут существенно отличаться по степени децентрализации, сложности инфраструктуры и уровням доверия к операторам. Централизованные мосты обеспечивают максимальную скорость и низкие издержки, но полностью зависят от одного участника, создавая единую точку отказа. Федеративные и ретрансляционные решения предполагают распределение ответственности, что снижает риски компрометации одного узла, но требует более сложных алгоритмов координации и синхронизации. Сайдчейн-мосты, легкие клиенты и zk-мосты обеспечивают более высокий уровень надежности, однако связаны с увеличением вычислительной нагрузки и повышенной сложностью реализации [2, 4]. Дополнительно стоит учитывать, что различные архитектуры сильно различаются по требованиям к инфраструктуре, затратам на эксплуатацию и совместимости с разными блокчейнами.

Существует несколько подходов к построению моделей безопасности кроссчейн-мостов. Одни решения опираются на мультиподписи и пороговые схемы, где для подтверждения межсетевых операций требуется согласие нескольких участников, что снижает вероятность атаки на единую точку отказа и создает дополнительный уровень надежности. Другие модели используют децентрализованные оракульные сети, которые собирают и агрегируют данные о событиях, происходящих в исходной цепи, и передают их целевой сети. Третье направление связано с применением встроенных легких клиентов, наследующих безопасность исходного протокола и позволяющих смарт-контрактам напрямую проверять корректность блоков. Наиболее строгие криптографические схемы опираются на zero-knowledge доказательства, позволяющие полностью исключить необходимость доверия к конкретным операторам [5]. Отдельное направление составляют оптимистичные мосты, где события считаются корректными «по умолчанию», но могут быть оспорены в течение challenge-периода, что создает дополнительный уровень децентрализации, но накладывает ограничения по времени финализации. Помимо этого, в экосистеме сохраняют актуальность централизованные модели с ручным

управлением активами и полностью децентрализованные P2P-решения на основе хеш-таймлоков (atomic swaps), которые позволяют пользователям напрямую обмениваться активами без посредников [6–8].

Несмотря на разнообразие решений, каждая архитектура сталкивается с собственным набором уязвимостей. Среди наиболее распространённых проблем — логические ошибки в смарт-контрактах, которые могут привести к несанкционированной эмиссии токенов или заморозке средств, криптографические изъяны в схемах верификации доказательств, наличие централизованных точек отказа, ненадежные механизмы управления ликвидностью и ошибки в расчетах обменных курсов, а также отсутствие инструментов автоматического мониторинга и экстренной приостановки операций [2–4]. Существенным риском является также недостаточный уровень формальной верификации: многие протоколы проходят только статический аудит и не охватывают полный набор сценариев, что особенно критично после доработки смарт-контрактов. Таким образом, даже при корректной изначальной архитектуре уязвимости могут появиться из-за отсутствия регулярного обновления и строгого контроля. Кроме того, экономические атаки и человеческий фактор, включая ошибки операторов и администраторов, остаются существенными источниками угроз.

Каждая из моделей демонстрирует уникальные компромиссы. ZK-протоколы предоставляют высокий уровень математической строгости и минимальное доверие к операторам, однако требуют значительных вычислительных ресурсов и имеют ограничения по совместимости с разными сетями [5]. Мультиподписи и пороговые схемы сравнительно просты в применении и хорошо известны, но их эффективность во многом зависит от правильной конфигурации параметров, надежного хранения ключей и дисциплины участников [6]. Легкие клиенты обеспечивают высокий уровень децентрализации, наследуя безопасность консенсуса исходной сети, но критически зависят от корректной и своевременной доставки заголовков блоков и Merkle-доказательств. Оракульные сети обладают хорошей масштабируемостью и удобны в использовании, но агрегаторы данных могут стать слабым звеном при компрометации или недостаточном уровне децентрализации. Оптимистичные мосты позволяют снизить доверие к централизованным участникам и расширяют спектр поддерживаемых сценариев, но характеризуются задержками в финализации транзакций и требуют активного мониторинга со стороны пользователей [7]. Атомарные свопы исключают необходимость в посредниках и обеспечивают полную децентрализацию процесса обмена, однако сталкиваются с проблемами ликвидности, поиска контрагентов и совместимости алгоритмов между разными цепями [8]. Все эти факторы подчеркивают, что выбор конкретной модели должен учитывать баланс между безопасностью, скоростью и затратами.

Перспективные направления развития включают улучшение zk-доказательств, усиление криптоэкономических стимулов и внедрение DAO-управления для большей прозрачности. Также важно формализовать аудиторские стандарты и внедрить единые процедуры проверки смарт-контрактов. Всё это позволит снизить количество ошибок и повысить устойчивость мостов к атакам.

Выбор архитектуры кроссчейн-мостов требует учета безопасности, скорости, затрат и масштабируемости. Современные тенденции показывают движение в сторону более децентрализованных и формализованных решений, которые могут обеспечить устойчивое развитие блокчейн-экосистемы.

#### СПИСОК ЛИТЕРАТУРЫ

1. Блокчейн мосты [Электронный ресурс] // Ethereum.org. URL: <https://ethereum.org/en/bridges/> (дата обращения: 20.07.2025).
2. Что такое блокчейн-мост и какие риски он в себе таит? [Электронный ресурс] // Habr. URL: <https://habr.com/ru/articles/709216/> (дата обращения: 20.07.2025).
3. Chainalysis: [официальный сайт] [Электронный ресурс]. URL: <https://www.chainalysis.com> (дата обращения: 20.07.2025).
4. Эксплойты кросс-чейн мостов: анализ рисков безопасности и пути развития DeFi [Электронный ресурс] // OKX Learn. URL: <https://www.okx.com/ru/learn/cross-chain-bridge-security-defi> (дата обращения: 20.07.2025).
5. ZK-мосты: Расширение возможностей кросс-чейн трансферов с использованием доказательств с нулевым разглашением [Электронный ресурс] // Medium / ScalingX. URL: <https://medium.com/@scalingx/zk-bridges-empowering-the-cross-chain-world-with-zero-knowledge-proofs-9e53eec91443> (дата обращения: 20.07.2025).
6. Мульти-подписи означают, что средства на мостах - это «одна маленькая оплошность» от взлома [Электронный ресурс] // Cointelegraph. URL: <https://cointelegraph.com/news/multisigs-mean-funds-in-bridges-are-one-small-slipup-from-being-hacked> (дата обращения: 20.07.2025).
7. Оптимистичные мосты [Электронный ресурс] // Medium / Connex. URL: <https://medium.com/connex/optimistic-bridges-fb800dc7b0e0> (дата обращения: 20.07.2025).
8. Что такое атомарные свопы [Электронный ресурс] // Chainlink Education Hub. URL: <https://chain.link/education-hub/atomic-swaps> (дата обращения: 20.07.2025).

УДК 004.8

#### ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ ДАННЫХ В ЛОКАЛЬНЫХ СЕТЯХ НА ОСНОВЕ БЛОКЧЕЙН-ТЕХНОЛОГИЙ

Шевяков Владислав Денисович<sup>1</sup>, Саенко Игорь Борисович<sup>2</sup>

<sup>1</sup> Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

<sup>2</sup> СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия

e-mails: vlad89312239540.la@yandex.ru, ibsaen@comsec.spb.ru

**Аннотация.** Технологии блокчейн предлагают инновационное решение для обеспечения целостности данных в корпоративных и локальных сетях благодаря децентрализованной структуре, неизменяемости записей и криптографической защите. Анализ показывает, что блокчейн обладает значительными преимуществами перед

традиционными централизованными системами, обеспечивая высокую устойчивость к подделке и несанкционированному доступу. Рассматриваются современные механизмы реализации — деревья Меркла, смарт-контракты, консенсусные алгоритмы, а также решения по повышению производительности: шардинг и Layer-2 технологии. Приведены практические примеры успешного внедрения, такие как KSI Blockchain и MediLedger. Интеграция с искусственным интеллектом и использование децентрализованных идентификаторов открывают новые перспективы для повышения безопасности и автоматизации процессов.

**Ключевые слова:** блокчейн, целостность данных; криптография; децентрализация; смарт-контракты; консенсусные алгоритмы.

## ENSURING DATA INTEGRITY IN LOCAL NETWORKS BASED ON BLOCKCHAIN TECHNOLOGIES

Shevyakov Vladislav<sup>1</sup>, Saenko Igor<sup>2</sup>

<sup>1</sup> Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny  
3 Tikhoretsky Av, St. Petersburg, 194064, Russia

<sup>2</sup> St. Petersburg Federal Research Center of the Russian Academy of Sciences  
39 14th Line VO, St. Petersburg, 199178, Russia  
e-mails: Vlad89312239540.la@yandex.ru, ibsaen@comsec.spb.ru

**Abstract.** Blockchain technologies offer an innovative solution for ensuring data integrity in corporate and local networks due to their decentralized structure, immutability of records, and cryptographic protection. The analysis shows that blockchain has significant advantages over traditional centralized systems, providing high resistance to tampering and unauthorized access. Modern implementation mechanisms are considered — Merkle trees, smart contracts, consensus algorithms, as well as performance-enhancing solutions: sharding and Layer-2 technologies. Practical examples of successful implementation are provided such as KSI Blockchain and the MediLedger platform. Integration with artificial intelligence and the use of decentralized identifiers open up new prospects for enhancing security and process automation.

**Keywords:** blockchain; data integrity; cryptography; decentralization; smart contracts; consensus algorithms.

Технологии блокчейн предлагают инновационное решение для обеспечения целостности данных в корпоративных и локальных сетях благодаря своей децентрализованной структуре и неизменяемости записей. Исследования показывают, что мировой рынок блокчейн-решений в финансовой сфере достигнет \$80,02 млрд к 2025 году, а в здравоохранении — \$7,04 млрд к 2030 году [1], что подчеркивает актуальность их внедрения.

Блокчейн обладает тремя ключевыми характеристиками: децентрализация, неизменяемость и криптографическая защита. Децентрализованная структура распределяет хранение данных между участниками сети, устраняя единую точку отказа и делая атаку экономически невыгодной. Неизменяемость обеспечивается за счет цепочки блоков, где каждый блок содержит хэш предыдущего — любое изменение данных приводит к расхождению хэшей и легко обнаруживается. Криптографические методы, такие как хэширование (SHA-256), цифровые подписи и консенсусные алгоритмы (Proof of Work, Proof of Stake), минимизируют риск подделки и двойного расходования данных [2].

В отличие от централизованных систем, где данные могут быть изменены администратором, блокчейн использует модель Append-Only Ledger — данные можно только добавлять, но не изменять. Управление доступом реализуется через приватные/публичные ключи и смарт-контракты, что обеспечивает более высокую безопасность по сравнению с традиционными моделями RBAC и ACL [3].

Современные решения включают деревья Меркла для эффективной проверки целостности данных, смарт-контракты для автоматизации процессов и консенсусные алгоритмы для достижения согласованности. Примером является внедрение платформы Hyperledger Fabric компанией Hitachi, предназначенной для управления цифровыми контрактами [4].

Особое внимание уделяется вопросам производительности. При увеличении числа устройств (например, в IoT-средах) возникают узкие места. Для решения используются шардинг, Layer-2 технологии (State Channels, Rollups) и edge computing, что позволяет достигать до 1200 транзакций в секунду. Тем не менее, такие системы, как Bitcoin (3–4 транз./сек) и Ethereum (15 транз./сек), пока уступают традиционным платежным системам [5].

Эффективное управление доступом обеспечивается с помощью разрешенных блокчейнов и децентрализованных идентификаторов (DID), позволяющих пользователям управлять своей цифровой идентичностью без посредников. Это снижает риски атак типа «Man-in-the-Middle» и повышает конфиденциальность [6].

Наиболее яркими примерами успешного внедрения блокчейн-технологии являются: система KSI Blockchain, применяемая для защиты медицинских данных, и платформа MediLedger, применяемая Baptist Health System и позволившая сэкономить около \$1 млн в год за счет оптимизации управления ценами и запасами [7]. Механизмы таймстемпинга обеспечивают точную фиксацию времени создания и изменения данных, что критично для аудита и юридических доказательств [8]. Интеграция с искусственным интеллектом позволяет анализировать поведение пользователей, выявлять аномалии и автоматически реагировать на подозрительную активность, повышая защищенность системы.

Перспективы развития включают совершенствование консенсусных алгоритмов, создание квантово-устойчивой криптографии и более глубокую интеграцию с системами машинного обучения, что позволит сделать процессы аудита и защиты данных еще более эффективными и надежными в будущем [9].

## СПИСОК ЛИТЕРАТУРЫ

1. Назаров А.В., Смирнов Е.А. Современные методы защиты данных в корпоративных сетях // Информационная безопасность. 2022. № 4. С. 45–58.
2. Петров Д.С. Блокчейн-технологии в финансовой сфере: рынок и перспективы развития // Финансовый менеджмент. 2023. № 2. С. 12–27.
3. Иванова М.Р. Применение блокчейна в здравоохранении: мировой опыт и прогнозы // Медицинские технологии. 2023. № 3. С. 78–92.
4. Кузнецов А.Н. Сравнительный анализ архитектур безопасности данных // Информационные технологии. 2023. № 1. С. 34–49.
5. Сидоров П.Е. Производительность блокчейн-систем при высоких нагрузках // Вычислительные технологии. 2022. № 5. С. 156–170.
6. Михайлов В.Г. Современные механизмы контроля доступа в распределенных системах // Безопасность информационных технологий. 2023. № 3. С. 89–104.
7. Алексеева Т.М. Аудит данных на базе блокчейн-технологий // Управленческий учет. 2022. № 4. С. 112–127.
8. Орлов Д.В. Практическое применение смарт-контрактов в бизнес-процессах // Автоматизация производства. 2023. № 2. С. 67–82.
9. Николаева Е.С. Перспективы развития блокчейн-технологий в корпоративном секторе // Экономика и менеджмент систем управления. 2023. № 6. С. 203–218.

УДК 004.451

**АНАЛИТИКА ЗАМЕНЯЕМОСТИ ОПЕРАЦИОННЫХ СИСТЕМ В ИНФОРМАТИЗАЦИИ  
ДИСЦИПЛИН ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА**

**Широков Владимир Владимирович, Щиголева Марина Андреевна**

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

Профессора Попова ул., 5, Санкт-Петербург, 197022, Россия

e-mails: vvshirokov@mail.ru, vvcehanovsky@mail.ru

**Аннотация.** Рассмотрен подход реализации в образовательном процессе профессиональной подготовки специалистов в области информационных технологий к решению конкретных задач профессиональной области и методология обучения. Обучение выстраивается в концепции приобретения и расширения собственного опыта на фундаменте сохранения научно обоснованного подхода в реализации основной профессиональной задачи. Выбраны разделы обеспечения безопасности операционных систем с пространствами имен, posix-возможностями, списками контроля доступа и безопасными вычислениями на примере использования ОС Ubuntu и рекомендуемой в настоящее время для проведения учебных занятий ОС Альт Образование.

**Ключевые слова:** компьютерная безопасность; безопасные вычисления; операционная система; пространства имен; posix-возможности.

**ANALYTICS OF REPLACEABILITY OF OPERATING SYSTEMS IN INFORMATIZATION  
OF DISCIPLINES OF THE EDUCATIONAL PROCESS**

**Shirokov Vladimir, Schigoleva Marina**

Saint Petersburg Electrotechnical University

5 Professor Popov St, St. Petersburg, 197022, Russia

e-mails: vvshirokov@mail.ru, vvcehanovsky@mail.ru

**Abstract.** Analytics of the replaceability of operating systems in the informatization of disciplines of the educational process. The approach of implementation in the educational process of professional training of specialists in the field of information technology to solve specific tasks of the professional field and the methodology of training are considered. Training is built in the concept of acquisition and expansion of own experience on the basis of preservation of a scientifically grounded approach in the implementation of the main professional task. The sections of ensuring the security of operating systems with namespaces, posix-capabilities, access control lists and secure calculations are selected on the example of using the Ubuntu OS and the Alt Education OS, which is currently recommended for conducting training classes.

**Keywords:** computer security; secure computing operating system; namespaces; posix capabilities.

Специфика образовательного процесса в области информационных технологий подразумевает необходимость обновления и взаимной замены программно-вычислительных средств решения однотипных задач и задач длительного использования. Мотивировка обновлений может быть связана с требованиями заявителя или заказчика задачи, необходимостью перехода на иную программно-вычислительную базу, на периодическую оценку эффективности применяемых средств при сравнении с другими вариантами реализации, универсальностью или уникальностью персонифицированной или корпоративной версий за счет, в том числе, вариантов программно-вычислительной и сервисной реализации. Во всех подобных случаях персонал разработчиков, администраторов и программистов должен быть готов к проведению работ, связанных с переходом на другие операционные системы и среды, языки описания и программирования, внешние библиотеки обращения.

Актуальность переходов на другие средства реализации и сопровождения основных процессов деятельности диктует необходимость профессионального решения этих задач, приобретения знаний, опыта, навыков, формирования необходимых методических подходов уже в ходе обучения профильных специалистов. Чем ближе род деятельности профессиональных задач к реальным производственным процессам, тем важнее роль практических тренингов и наличия навыков в решении конкретных задач профессиональной области. Методология обучения выстраивается на приобретении и расширении собственного опыта на фундаменте

сохранения научно обоснованного подхода и целевой установки, в соответствии с которой возникает конкретная производственная или исследовательская задача.

Подход к формированию навыков работы специалистов в области информационных технологий для задач обновления базовой операционной системы ОС Ubuntu на ОС Альт Образование показан на примере обновлений, касающихся обеспечения информационной безопасности средств операционной системы. Эти разделы включены в практические задания профессиональной подготовки разработчиков, администраторов и программистов и удовлетворяют образовательным рекомендациям по применению отечественных операционных систем.

В настоящее время рекомендуемой для использования в учебном процессе является отечественная операционная система Альт Образование [1]. Перевод практических занятий с традиционно используемой ОС Ubuntu на рекомендуемую ОС Альт Образование потребовал обновить методические указания для проведения практических работ. А также выделить тематические разделы, требующие отражения конкретных разделов дисциплин подготовки. Обновление коснулось разделов, относящихся к вопросам безопасности операционных систем: пространства имен, posix-возможности, списки контроля доступа, безопасные вычисления. Задания построены таким образом, чтобы в равной степени отражать аналитическую необходимость и целесообразность решения задачи и формирование конкретных навыков по их технической реализации.

Было проверено в пространствах имен PID, UTS, TIME, USER, меняется ли состав команд при проверке свойств изолированности пространств имен. Наибольшее различие выявлено в функциональности пространства имен USER, что требует дальнейшего изучения, в том числе и для других пространств NETWORK, MOUNT и CGROUP [2].

Были рассмотрены особенности чтения и установки posix-возможностей в ОС Ubuntu и ОС Альт Образование. При установке библиотеки для работы с posix-возможностями в Ubuntu необходимо набирать команду `sudo apt install libcap-dev`. При установке библиотеки с такой же функциональностью в Альт Образование необходимо набирать команду `sudo apt-get install libcap-devel`. То есть различие имеется в именах библиотек поддержки posix-возможностей [3].

При рассмотрении особенностей чтения и формирования списков контроля доступа в ОС Ubuntu и ОС Альт Образование также есть различие. В ОС Ubuntu устанавливается библиотека `libacl-dev`, в ОС Альт Образование устанавливается библиотека `libacl-devel`. То есть различие имеется в именах библиотек для поддержки списков контроля доступа [4].

При реализации безопасных вычислений были выявлены особенности обеих ОС: в ОС Ubuntu необходимо устанавливать библиотеку `libseccomp-dev` для поддержки программирования безопасных вычислений, в ОС Альт Образование библиотека с такой же функциональностью называется `libseccomp-devel`.

Таким образом, образовательный цикл подготовки включает аналитическую часть - сравнение средств для работы с механизмами обеспечения безопасности двух ОС — Ubuntu и Альт Образование. Результаты сравнения показывают, что средства двух ОС в основном совпадают, различаются имена библиотек, поддерживающих программирование с использованием соответствующих механизмов. У учащихся остается полезный навык практической реализации конкретной задачи предметной области профессиональной подготовки.

#### СПИСОК ЛИТЕРАТУРЫ

1. Альт Образование. Операционная система для тех, кто учится и учит [электронный ресурс] URL: <https://www.basealt.ru/alt-education> (дата обращения: 12.06.2025).
2. Изоляция процессов и минимизация привилегий: Linux namespaces и seccomp [электронный ресурс] URL: <https://selectel.ru/blog/namespaces-and-seccomp> (дата обращения: 15.05.2025).
3. Разрешения POSIX для файлов: Разделяем полномочия root [электронный ресурс] URL: <https://www.linux.org.ru/news/doc/2444070/seccomp> (дата обращения: 19.06.2025).
4. Скабцов Н. В. Kali Linux в действии. Аудит безопасности информационных систем. СПб.: Питер, 2024. 384 с. (Серия «Библиотека программиста»).

УДК 004.056.5

#### ВОССТАНОВЛЕНИЕ КРИПТОГРАФИЧЕСКОГО КЛЮЧА ИЗ ИЗОБРАЖЕНИЯ РАДУЖНОЙ ОБОЛОЧКИ С ИСПОЛЬЗОВАНИЕМ НЕЙРОСЕТЕВОЙ МОДЕЛИ

Штука Станислав Евгеньевич, Боршевников Алексей Евгеньевич

Дальневосточный федеральный университет

п. Аякс, 10, о. Русский, г. Владивосток, Приморский край, 690922, Россия

e-mail: [shtuka.se@dvfu.ru](mailto:shtuka.se@dvfu.ru)

**Аннотация.** В работе представлен подход к высоконадёжной биометрической аутентификации по радужной оболочке глаза. Предложенная архитектура сочетает сегментацию радужки с использованием U-Net, нормализацию изображения (метод Даугмана и кадрирование), а также восстановление бинарного ключа фиксированной длины на основе свёрточной сети DenseNet121 и многослойного персептрона. Модель обучается восстанавливать фиксированные ключи для образцов «свой» и формировать непредсказуемые коды для «чужих». Эксперименты показали, что при использовании кадрирования достигается Ассигасу в 94,4% при нулевом уровне FAR, что подтверждает надёжность предложенного подхода.

**Ключевые слова:** радужная оболочка глаза; биометрия; высоконадёжная аутентификация; извлечение признаков; восстановление ключа; CNN; расстояние Хэмминга.



## RECONSTRUCTION OF A CRYPTOGRAPHIC KEY FROM AN IRIS IMAGE USING A NEURAL NETWORK MODEL

Shtuka Stanislav, Borshevnikov Aleksey

Far Eastern Federal University

10 Ajax, Russky Island, Vladivostok, Primorsky Krai, 690922, Russia

e-mail: shtuka.se@dvfu.ru

**Abstract.** This work presents an approach to highly reliable biometric authentication based on iris recognition. The proposed architecture integrates iris segmentation using U-Net, image normalization (Daugman's method and cropping), and binary key reconstruction with a pre-trained DenseNet121 combined with a multilayer perceptron. The model is trained to reproduce fixed keys for «genuine» samples and generate unpredictable codes for «impostors». Experimental results show that cropping-based normalization achieves an Accuracy of 94.4% with zero FAR, confirming the reliability of the proposed approach.

**Keywords:** iris recognition; biometric authentication; key reconstruction; feature extraction; convolutional neural network; Hamming distance.

Современные требования к безопасности информационных систем предъявляют повышенные стандарты к биометрическим методам аутентификации. Среди них особое место занимает аутентификация по радужной оболочке глаза, обладающая высокой уникальностью и стабильностью. Однако практическое применение таких систем осложняется вариативностью условий съёмки, шумами и необходимостью криптографической защиты биометрических данных.

В представленной работе предлагается решение задачи восстановления криптографически пригодного бинарного ключа фиксированной длины из изображения радужной оболочки. В отличие от традиционных методов, оперирующих шаблонами признаков и классическими классификаторами (SVM, k-NN и др.), в данном подходе ключевой акцент сделан на построении нейросетевой архитектуры, которая объединяет извлечение признаков и восстановление бинарного кода.

Алгоритм включает следующие этапы:

1. Сегментацию радужной оболочки с использованием U-Net [1].
2. Нормализацию изображения. В рамках работы рассмотрены два варианта: разворачивание по Даугману [2] и метод кадрирования.
3. Извлечение признаков и восстановление ключа. Предобученная DenseNet121 использовалась как экстрактор признаков, а многослойный персептрон восстанавливал 256-битный бинарный ключ.
4. Аутентификацию. Проверка совпадения ключей выполнялась через расстояние Хэмминга с заданным порогом.

Бинарные коды для «своих» пользователей заранее формировались случайным образом. Модель обучалась на парах «нормализованное изображение «своего» – соответственный бинарный ключ», что позволяет для «своих» восстанавливать фиксированный ключ, а для «чужих» генерировать непредсказуемые коды.

Эксперименты показали, что использование кадрирования в качестве метода нормализации обеспечивает наилучшие результаты: Ассигасу – 94,4%, FRR – 7,14%, FAR – 0% при длине ключа 256 бит и пороге Хэмминга 32. Для нормализации по Даугману результаты оказались хуже (Ассигасу – 73,7%, FRR – 33,7%, FAR – 0%).

При этом классические классификаторы на CNN-признаках (SVM, k-NN, Random Forest) демонстрируют Ассигасу до 99,7% [3], однако они не решают задачу построения криптографически пригодного ключа и не соответствуют требованиям высоконадёжной аутентификации [4, 5].

Таким образом, предложенный подход позволяет совмещать биометрию и криптографию: решает задачу восстановления устойчивого бинарного ключа из изображения радужной оболочки.

Полученные результаты подтверждают применимость модели в задачах высоконадёжной аутентификации, где критически важно низкое значение ошибки второго рода (FAR) при приемлемом уровне ошибки первого рода (FRR). Перспективным направлением развития работы является расширение обучающих выборок, повышение точности сегментации и исследование альтернативных архитектур модели для восстановления ключа.

## СПИСОК ЛИТЕРАТУРЫ

1. Ronneberger O., Fischer P., Brox T. U-net: Convolutional networks for biomedical image segmentation // Medical image computing and computer-assisted intervention–MICCAI: 18th international conference, Munich, Germany, October 5-9, 2015, proceedings, part III 18. Springer International Publishing, 2015. С. 234-241.
2. Daugman J. How iris recognition works // The essential guide to image processing. Academic Press, 2009. С. 715-739.
3. Ganeeva Y. K., Myasnikov E. V. Identifying persons from iris images using neural networks for image segmentation and feature extraction // Computer Optics. 2022. Т. 46. № 2. С. 308-316.
4. ГОСТ Р. 52633.0-2006: Защита информации // Техника защиты информации. Требования к средствам высоконадёжной биометрической аутентификации, 2007.
5. ГОСТ Р. 52633.5-2011 Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрии - код доступа, 2011.

УДК 004.27+004.056

**ПРИНЦИПЫ ПОСТРОЕНИЯ ОТКАЗОУСТОЙЧИВЫХ И ЗАЩИЩЁННЫХ АРХИТЕКТУР ГИС  
ДЛЯ ПОДДЕРЖКИ АДАПТИВНЫХ ПРОЕКТНЫХ РЕШЕНИЙ В МЧС РОССИИ****Грызунов Виталий Владимирович<sup>1</sup>, Сагитов Азат Альфредович<sup>2</sup>**<sup>1</sup> Санкт-Петербургский университет ГПС МЧС России  
Московский пр., 149, Санкт-Петербург, 196105, Россия<sup>2</sup> Главное управление МЧС России по Мурманской области  
Шабалина ул., 8, Мурманск, 183052, Россия  
e-mails: viv1313r@mail.ru, sagitov-2014@mail.ru

**Аннотация.** Рассматриваются технические и организационные принципы построения архитектур ГИС, обеспечивающих одновременно отказоустойчивость, информационную безопасность и поддержку адаптивного управления проектами в системе МЧС России.

**Ключевые слова:** ГИС; информационная безопасность; отказоустойчивость; адаптивное управление; чрезвычайные ситуации; МЧС России; защищённая архитектура; проектное управление.

**PRINCIPLES OF BUILDING FAULT-RESISTANT AND PROTECTED GIS ARCHITECTURES  
TO SUPPORT ADAPTIVE DESIGN SOLUTIONS IN THE EMERCOM OF RUSSIA****Gryzunov Vitaly<sup>1</sup>, Sagitov Azat<sup>2</sup>**<sup>1</sup> Saint-Petersburg State Fire Service University of the Ministry of the Russian Federation for Civil Defense,  
Emergencies and Elimination of Consequences of Natural Disasters  
named after the Hero of the Russian Federation Army General E. N. Zinichev  
149 Moskovsky Av, St. Petersburg, 196105, Russia<sup>2</sup> The Main Directorate of the Russian Ministry of Emergency Situations in the Murmansk region  
8 Shabalina St, Murmansk, 183052, Russia  
e-mails: viv1313r@mail.ru, sagitov-2014@mail.ru

**Abstract.** The article discusses the technical and organizational principles of building GIS architectures that simultaneously ensure fault tolerance, information security, and support for adaptive project management in the Russian Ministry of Emergency Situations.

**Keywords:** GIS; information security; fault tolerance; adaptive management; emergency situations; the Russian Ministry of Emergency Situations; secure architecture; project management.

В условиях роста масштабов, сложности и непредсказуемости чрезвычайных ситуаций (ЧС) природного и техногенного характера геоинформационные системы (ГИС) становятся критически важным инструментом для оперативного принятия решений, координации действий и управления ресурсами. Однако высокая динамика ЧС, нестабильность инфраструктуры и возрастающие киберугрозы требуют от ГИС не только функциональной гибкости, но и устойчивости к сбоям и атакам. В докладе рассматриваются технические и организационные принципы построения архитектур ГИС, обеспечивающих одновременно отказоустойчивость, информационную безопасность (ИБ) и поддержку адаптивного управления проектами в МЧС России [1–4]. Основные положения перечислены ниже.

*Адаптивность как ключевое требование к ГИС в ЧС.*

Адаптивное управление проектами МЧС России предполагает быструю перестройку планов, перераспределение ресурсов и изменение тактики в ответ на меняющуюся обстановку.

ГИС должна обеспечивать оперативный доступ к актуальным пространственным данным, поддерживать моделирование сценариев и визуализацию в реальном времени.

Эффективность адаптации ГИС к дестабилизирующим факторам может быть оценена с помощью специализированных нестохастических показателей, отражающих «полезность» системы для пользователя в кризисных условиях [2].

*Угрозы и вызовы для ГИС в условиях ЧС:*

- Физические повреждения инфраструктуры (электропитание, связь).
- Кибератаки — DDoS, подмена данных, компрометация источников геоданных.
- Нарушение целостности и достоверности пространственной информации.
- Высокая зависимость от внешних сервисов (например, спутниковых снимков, облачных платформ).

Наиболее опасными с точки зрения экспертов признаны уязвимости, связанные с недостаточной проверкой входных данных, инъекциями, нарушениями аутентификации и управления доступом, а также ошибками конфигурации ПО [1].

Для адекватного противодействия злоумышленникам необходимо использовать модели их агрессивных действий, позволяющие оценивать потенциал воздействия без привязки к вероятностным распределениям [6].

*Принципы отказоустойчивой архитектуры ГИС.*

- Модульность и микросервисная архитектура: изоляция компонентов для локализации сбоев.
- Репликация и резервирование данных: географически распределённые копии критически важных слоёв.

- Оффлайн-режим и edge-вычисления: возможность работы при потере связи с центром; граничные вычисления признаны предпочтительной платформой для распределённых ИС критического применения [1].
- Автоматическое восстановление: self-healing механизмы и быстрое переключение на резервные узлы.
- Адаптивное управление доступностью ресурсов за счёт агрегирования производительности физических элементов в виртуальные пулы и перераспределения внутренних резервов задач позволяет вдвое снизить риски, связанные с нарушением доступности [4].

В условиях деградации ИВС допустимо снижать требования к производительности за счёт временных резервов и допустимых погрешностей, что особенно актуально для ГИС в длительных ЧС [5].

*Принципы защищённой архитектуры ГИС:*

- Многоуровневая защита: от периметра (сетевой экран) до данных (шифрование, цифровые подписи).
- Контроль целостности геоданных: использование хеш-цепочек и блокчейн-подобных механизмов для верификации источников.
- Разграничение доступа на основе ролей и контекста: динамические политики ИБ в зависимости от уровня угрозы и статуса ЧС.
- Аудит и мониторинг в реальном времени: выявление аномалий в использовании ГИС и подозрительных запросов.

Для обеспечения доверия при интеграции распределённых компонентов ГИС рекомендуется применять модели доверия, основанные на инфраструктуре открытых ключей и электронной подписи, с учётом специфики систем критического применения [3].

Приоритетными аспектами ИБ для таких систем эксперты называют доступность, аутентичность и целостность именно они должны лежать в основе архитектурных решений [1].

*Организационные аспекты:*

- Интеграция требований ИБ и отказоустойчивости в жизненный цикл проектов МЧС России.
- Обучение персонала работе с ГИС в условиях компрометации или сбоя.
- Разработка регламентов взаимодействия между ИТ-службами, аналитиками и оперативными группами.
- Тестирование архитектуры через учения и «красно-синие» команды.

Использование нестохастических моделей агрессивных действий [6] и методик снижения требований к производительности в условиях деградации [5] позволяет повысить устойчивость управленческих процессов даже при частичной компрометации ГИС.

Таким образом эффективное адаптивное управление в условиях ЧС невозможно без надёжной и безопасной геоинформационной инфраструктуры. Предложенные принципы позволяют построить ГИС, которая не только выдерживает экстремальные нагрузки и киберугрозы, но и остаётся гибким инструментом поддержки управленческих решений. Дальнейшие исследования целесообразно направить на стандартизацию таких архитектур и их интеграцию в единое информационное пространство МЧС России.

#### СПИСОК ЛИТЕРАТУРЫ

1. Грызунов В. В., Гришечко А. А., Сипович Д. Е. Выбор Наиболее опасных уязвимостей для перспективных информационных систем критического применения // Вопросы кибербезопасности. 2022. № 1(47). С. 66–75.
2. Burlov V. G., Gryzunov V. V. Evaluation of the effectiveness of geographic information systems adaptation to destabilizing factors // Journal of Physics: Conference Series. 2020. P. 012016.
3. Грызунов В. В., Корниенко А. А., Глухарев М. Л., Крюков А. С. Выбор моделей доверия при интеграции распределённых информационных систем критического применения // Проблемы информационной безопасности. Компьютерные системы. 2021. № 4. С. 79–90.
4. Грызунов В. В. Методы адаптивного управления доступностью ресурсов геоинформационных систем в условиях деструктивных воздействий // Труды учебных заведений связи. 2022. Т. 8, № 3. С. 101–116.
5. Грызунов В. В. Методика решения измерительных и вычислительных задач в условиях деградации информационно-вычислительной системы // Вестник СибГУТИ. 2015. № 1(29). С. 35–46.
6. Грызунов В. В. Модель целенаправленных агрессивных действий на информационно-вычислительную систему // Человеческий фактор в сложных технических системах и средах (Эрго-2018). СПб., 2018. С. 300–305.



## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

УДК 004.056

### НАПРАВЛЕНИЯ АВТОМАТИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ

**Авраменко Владимир Семенович**

Военная академия связи им. Маршала Советского Союза С. М. Буденного  
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия  
e-mail: vsavr@yandex.ru

**Аннотация.** Рассмотрена проблема автоматизации защиты информации в инфокоммуникационных системах, представлены основные направления автоматизации функций и задач защиты информации.

**Ключевые слова:** инфокоммуникационная система; защита информации; автоматизация; оперативность; машинное обучение.

### DIRECTIONS OF AUTOMATION OF INFORMATION PROTECTION IN INFORMATION AND COMMUNICATION SYSTEMS

**Avramenko Vladimir**

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny  
3 Tikhoretsky Av, St. Petersburg, 194064, Russia  
e-mail: vsavr@yandex.ru

**Abstract.** The article discusses the problem of automating information protection in information and communication systems and presents the main directions for automating information protection functions and tasks.

**Keywords:** infocommunication system; information security; automation; efficiency; machine learning.

Проблема защиты информации в инфокоммуникационных системах в настоящее время резко обострилась, о чем свидетельствует рост количества успешных атак на инфокоммуникационные системы различного назначения, в том числе и относящихся к объектам критической инфраструктуры. К основным факторам, обусловившим обострение проблемы защиты, относятся следующие:

- рост количества и сложности атак;
- последствия ухода с отечественного рынка ведущих зарубежных производителей средств автоматизации и защиты информации;
- расширение номенклатуры средств защиты информации;
- дефицит квалифицированных кадров в области информационной безопасности;
- рост затрат на подготовку и оплату услуг специалистов по защите информации;
- значительное количество задач защиты информации, выполняемых вручную.

Последний фактор следует отнести к наиболее существенным в сложившейся ситуации, так как в современных условиях функционирования инфокоммуникационных систем время выполнения выполняемых вручную ряда важных задач по защите информации становится недопустимо большим. Кроме того, человеческий фактор неизбежно порождает ошибки при принятии и реализации решений, проблемы взаимодействия на организационном уровне.

К числу проблемных (по оперативности выполнения и достоверности принимаемых решений) следует отнести задачи анализа защищенности инфокоммуникационной системы, диагностирования обнаруженных нарушений безопасности и выработки решения на реагирование. Очевидным путем повышения эффективности защиты является автоматизация решения сложных, трудоемких и рутинных задач.

На уровне управления защитой информации в первую очередь необходимо повышать степень автоматизации реализации таких функций управления, как сбор и обработка данных о защите, контроль (оценка) состояния защищенности, выработка решений по восстановлению защищенного состояния. На уровне средств защиты необходимо стремиться к автоматической реализации функций диагностирования обнаруженных попыток и фактов нарушений безопасности, оперативного прогнозирования траекторий развития атак, проведения мероприятий по реагированию, настройки средств защиты. В перспективе целесообразно ориентироваться на создании автоматизированной системы защиты инфокоммуникационной системой, как целостной совокупности взаимосвязанных персонала, средств и технологий защиты.

Перспективным направлением автоматизации защиты информации является применение технологий машинного обучения для выполнения трудоемких и сложных задач защиты [1–3]. К таким задачам в первую

очередь относятся обработка больших объемов разнородной информации о состоянии защиты, анализ защищенности, прогнозирование защищенности, обнаружение сложных атак, поддержка принятия решений.

#### СПИСОК ЛИТЕРАТУРЫ

1. Как искусственный интеллект повышает кибербезопасность [Интернет-ресурс]. URL: [www.rbc.ru/neweconomy/news/6554cc119a79477fa20d3dda](http://www.rbc.ru/neweconomy/news/6554cc119a79477fa20d3dda) (дата обращения: 08.09.2025).
2. Искусственный интеллект и машинное обучение в кибербезопасности — прогноз на будущее [Интернет-ресурс]. URL: [www.kaspersky.ru/resource-center/definitions/ai-cybersecurity](http://www.kaspersky.ru/resource-center/definitions/ai-cybersecurity) (дата обращения: 19.02.2024).
3. Авраменко В. С. Анализ защищенности компьютерных сетей с применением технологий искусственного интеллекта // Актуальные проблемы защиты и безопасности: Труды XXVII Всероссийской научно-практической конференции. СПб: РАРАН, 2024. С. 287-290.

УДК 004.056

### ПРОГРАММНЫЙ КОМПЛЕКС ОПРЕДЕЛЕНИЯ МЕСТОПОЛОЖЕНИЯ ИСТОЧНИКОВ ВНУТРЕННИХ НАРУШЕНИЙ БЕЗОПАСНОСТИ В ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ

Авраменко Владимир Семенович

Военная академия связи им. Маршала Советского Союза С. М. Буденного  
Тихорецкий пр-т, д. 3, Санкт-Петербург, 194064, Россия  
e-mail: vsavr@yandex.ru

**Аннотация.** Предлагается способ автоматизированного определения физического местоположения внутреннего нарушителя безопасности информации на основе анализа данных о состоянии сетевого оборудования с использованием программного комплекса.

**Ключевые слова:** вычислительная сеть; нарушение безопасности; местоположение; программный комплекс; автоматизация.

### SOFTWARE COMPLEX FOR DETERMINING THE LOCATION OF INTERNAL SECURITY VIOLATIONS IN COMPUTER NETWORKS

Avramenko Vladimir

Military Academy of Communications Marshal of the Soviet Union S.M. Budyonny  
Tikhoretsky Ave., 3, St. Petersburg, 194064, Russia  
e-mail: vsavr@yandex.ru

**Abstract.** The invention proposes a method for automatically determining the physical location of an internal information security breacher based on the analysis of network equipment status data using a software package.

**Keywords:** computing network; security breach; location; software package; automation.

Одной из задач, решаемых в ходе диагностирования внутренних нарушений безопасности в вычислительных сетях различного назначения, является оперативное определение физического местоположения внутреннего нарушителя для обеспечения своевременного и адекватного реагирования.

В нормативных документах по реагированию на компьютерные инциденты, исследованиях по их локализации данному вопросу уделяется недостаточно внимания, так как в большей степени они ориентированы на внешнего нарушителя и считается, что при обнаружении нарушения в большинстве случаев достаточно ограничить доступ к объекту атаки путем блокировки IP-адреса нарушителя [1, 2].

Но в некоторых случаях такой вариант реагирования может не привести к положительному результату (например, нарушитель может продолжить атаку с другим IP-адресом или принять меры по сокрытию реальных сетевых параметров) и требуется определить точное физическое положение нарушителя для локализации нарушения.

На практике местоположение источника нарушения безопасности в большинстве случаев осуществляется администраторами вручную с использованием различных стандартных утилит. Но если в небольших сетях источник обнаружить и локализовать можно достаточно просто и быстро стандартными способами, то для большой и территориально распределенной вычислительной сети задача оперативного поиска физического местоположения источника нарушения становится сложной, может выполняться недопустимо длительное время.

Для решения данной задачи предлагается способ автоматизированного определения местоположения источников нарушения безопасности на основе программного комплекса, основной функцией которой является отслеживание в близком к реальному масштабу времени местоположения конечных сетевых устройств на основе анализа информации о состоянии коммутационного оборудования.

Суть предлагаемого способа заключается в сканировании SNMP-устройств, кэшировании полученной информации на сервере и автоматическом сопоставлении полученных данных с информацией о физическом местоположении сетевого оборудования, что позволяет постоянно отслеживать физическое местоположение абонентов в сети, а также их перемещение.

Программный комплекс определения местоположения источника нарушения безопасности может использоваться как самостоятельно, так и в составе автоматизированной системы диагностирования нарушений безопасности [3]. Кроме того, предлагаемый способ может использоваться для реализации вспомогательного

механизма аутентификации абонентов сети по их местоположению, а также в качестве дополнительного источника данных о пользователях в системах аутентификации на основе методов машинного обучения [4].

Применение администраторами безопасности программного комплекса автоматизации определения местоположения внутреннего источника нарушений безопасности позволит обеспечить более оперативное и адекватное реагирование на нарушения безопасности и другие компьютерные инциденты, обусловленные неполадками в сети.

#### СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 59711-2022. Защита информации. Управление компьютерными инцидентами. Организация деятельности по управлению компьютерными инцидентами.
2. Кузнецов, А. В. Модели данных для автоматизации реагирования на инциденты / А. В. Кузнецов // Безопасность информационных технологий. 2025. Т. 32, № 2. С. 48-58. DOI 10.26583/bit.2025.2.04. EDN VFXSOK.
3. Авраменко В. С., Маликов А.В. Оценка эффективности диагностирования компьютерных инцидентов в инфокоммуникационных системах // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. Т. 2 / под ред. С.В. Бачевского. СПб.: СПбГУТ, 2021. С. 10-15.
4. Авраменко В. С., Маликов А.В. Подход к аутентификации пользователей инфокоммуникационных систем с применением машинного обучения // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. Т. 2 / под ред. С.В. Бачевского. СПб.: СПбГУТ, 2020. С. 13-17.

УДК 004.056

### ПРОГНОЗИРОВАНИЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ НА ОСНОВЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ

Авраменко Владимир Семенович, Орлов Алексей Сергеевич

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: vsavr@yandex.ru, toretto08021993@yandex.ru

**Аннотация.** Рассматривается проблема прогнозирования защищенности информации в автоматизированных системах. Представлены некоторые подходы к прогнозированию защищенности информации в автоматизированных системах на основе методов машинного обучения.

**Ключевые слова:** автоматизированная система; защищенность информации; угроза; прогнозирование защищенности; метод прогнозирования; машинное обучение.

### FORECASTING THE PROTECTION OF INFORMATION IN AUTOMATED SYSTEMS

Avramenko Vladimir, Orlov Aleksei

Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: vsavr@yandex.ru, toretto08021993@yandex.ru

**Abstract.** The problem of forecasting information security in automated systems is considered. Some approaches to forecasting information security in automated systems based on machine learning methods are presented.

**Keywords:** automated system; information security; threat; security forecasting; forecasting method; machine learning.

Одной из ключевых проблем обеспечения эффективного функционирования автоматизированных систем является проблема защиты информации от несанкционированного доступа и компьютерных атак. Проблема защиты информации относится к классу постоянных. Несмотря на активное совершенствование и развитие средств и технологий защиты информации, регулярно появляются сообщения о неправомерных действиях с защищаемой информацией в автоматизированных системах различного назначения. Более того, анализ общедоступной статистики нарушений свидетельствует о росте числа компьютерных атак, что является симптомом обострения проблемы защиты информации.

Основные причины, обуславливающие возможность реализации угроз безопасности информации в автоматизированных системах общего и специального назначения:

- использование общего и прикладного программного обеспечения общего назначения, имеющего уязвимости;
- ограничения на обновление программного обеспечения иностранного производства;
- ограниченные вычислительные ресурсы для развертывания современных средств защиты информации;
- расположение отдельных компонентов системы за пределами контролируемых зон;
- арендуемые каналы обмена данными с взаимодействующими системами;
- наличие открытых для общего доступа сетевых ресурсов;
- использование беспроводных технологий передачи данных и мобильных технических средств;
- использование незащищенных протоколов передачи информации.

Следует отметить, что в последнее время на фоне сложившейся геополитической ситуации резко повисла активность внешних нарушителей безопасности информации.

Также опасными источниками угроз безопасности информации в автоматизированных системах являются администраторы и пользователи, имеющие непосредственный доступ к компонентам АС, а также администраторы и пользователи взаимодействующих АС. Кроме того, опасным источником угроз являются вредоносные аппаратные и программные средства, внедренные в АС на стадии создания или эксплуатации.

В связи с постоянно возрастающими возможностями нарушителей и высокой динамикой реализации угроз безопасности информации защита в современных АС должна носить упреждающий характер. В свою очередь, действительно упреждающая защита требует реализации функции прогнозирования защищенности информации. Основной целью прогнозирования защищенности является создание запаса времени для проведения мероприятий превентивного характера на возможные отдельные атаки и нарушение защищенного состояния автоматизированной системы.

При прогнозировании защищенности в качестве прогнозных величин могут использоваться тип и продолжительность возможной или начинающейся атаки, количество и интенсивность появления уязвимостей и источников атак, величина потенциального ущерба и другие частные показатели. А для принятия обоснованных решений по защите информации в автоматизированной системе в целом целесообразно использовать комплексные показатели защищенности, учитывающие как процессы нарушения безопасности, так и процессы восстановления защищенного состояния [1].

В существующих системах защиты информации автоматизированных систем прогнозирование защищенности информации практически не осуществляется, а предлагаемые средства автоматизированного прогнозирования как отдельных атак, так и уровня защищенности информации в автоматизированной системе в целом, недостаточно эффективны. Основной причиной проблемы прогнозирования защищенности информации в автоматизированных системах является невысокая результативность (точность прогнозирования) и низкая степень автоматизации решений на основе традиционных прогнозных аналитических и статистических моделей защищенности.

Перспективным путем решения проблемы прогнозирования защищенности информации в автоматизированных системах является применение методов машинного обучения, активно развивающихся и успешно использующихся на практике в различных областях деятельности. В настоящее время в этом направлении исследования проводятся достаточно активно.

В частности, в [2] для прогнозирования количества инцидентов предлагается использовать метод *k*-ближайших соседей. В [3] представлена методика прогнозирования сетевых компьютерных атак на основе определения весов атрибутов сетевой компьютерной атаки с применением метода дерева принятия решений, включая математический аппарат ее реализации, также приведена структура программного модуля, в котором предлагаемая методика реализована.

Одним из перспективных направлений повышения эффективности прогнозирования защищенности на основе методов машинного обучения является использование рекуррентных сетей с ячейками Long Short-Term Memory (LSTM) или GRU-сетей [4].

Для достижения максимальной точности прогноза защищенности информации в автоматизированной системе при наличии достаточно полных и достоверных исходных данных за длительные периоды времени более предпочтительным представляется использование LSTM-сетей. В условиях ограниченности статистических данных о функционировании автоматизированной системы в прошлом и (или) жестких ограничений на вычислительные ресурсы целесообразно использовать GRU-сети.

Результаты известных исследований показывают, что прогнозные модели на основе методов машинного обучения более точны в задачах прогнозирования показателей защищенности, чем классические статистические модели. В свою очередь, к недостаткам известных подходов к прогнозированию защищенности на основе методов машинного обучения следует отнести сложность их применения на практике, что обусловлено низкой степенью автоматизации. Большинство предлагаемых решений разработаны на уровне программных макетов, требующих достаточно высокой квалификации и большого количества ручной работы по сбору и подготовке исходных данных, настройке и обучению моделей.

Таким образом, разработка и внедрение средств и технологий автоматизированного прогнозирования защищенности на основе методов машинного обучения является перспективным направлением повышения эффективности прогнозирования как отдельных атак и угроз, так и уровня защищенности информации в автоматизированной системе в целом, требует более детальной проработки и реальной практической апробации.

#### СПИСОК ЛИТЕРАТУРЫ

1. Авраменко В.С., Тарасов А.В. Прогнозирование защищенности информации в автоматизированных системах специального назначения // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. Т.2. С. 19-24.
2. Беляева Т.А., Микрюков А.А. Нейросетевое прогнозирование инцидентов информационной безопасности // Международный студенческий научный вестник. 2023. № 6. С. 30.
3. Алпеев Е.В., Стадник А.Н., Скрыль С.В. Методика прогнозирования компьютерных атак на основе определения весов атрибутов компьютерной атаки с применением метода деревьев решений / Научные труды КубГТУ. 2021. № 6. С. 82-92
4. Авраменко В. С., Саенко И. Б., Котенко И. В. Прогнозная модель защищенности информации в инфокоммуникационных системах на основе рекуррентной нейронной сети // Правовая информатика 2025. № 2. С. 153-160.

УДК 004.94+519.2+681.5

**ГЕОКОНТРОЛЛИНГ: ПОДХОДЫ К РЕАЛИЗАЦИИ ПОДДЕРЖКИ УПРАВЛЕНИЯ  
ТЕРРИТОРИАЛЬНОЙ АКТИВНОСТЬЮ****Звездарёв Дмитрий Валентинович, Ефремов Дмитрий Александрович, Биденко Сергей Иванович,  
Беляев Александр Константинович**АО «Научно-производственное объединение «Импульс»  
Киришская ул., 2, Санкт-Петербург, 195299, Россия  
emails: proimpuls@peterlink.ru

**Аннотация.** Описываются принципы построения систем геоконтроллинга регионом как реализация автоматизированной поддержки управления территориальными объектами и системами.

**Ключевые слова:** региональная хозяйственная и социальная активность, автоматизированное управление территорией, киберспособность системы управления территорией, активность карты, хорологизация, топологизация, геосистемность, интермодальность

**GEOCONTROLLING: APPROACHES TO THE IMPLEMENTATION OF SUPPORT  
FOR THE MANAGEMENT OF TERRITORIAL ACTIVITY****Zvezdarev Dmitry, Efremov Dmitry, Bidenko Sergey, Belyaev Alexander**Joint Stock Company «Scientific and Production Association «Impulse»  
2 Kirishskaya St, St. Petersburg, 195299, Russia  
emails: proimpuls@peterlink.ru

**Abstract.** The principles of building geocontrolling systems by the region as the implementation of automated support for the management of territorial objects and systems are described.

**Keywords:** regional economic and social activity, automated management of the territory, cyberability of the territory management system, map activity, chorologization, topologization, geosystemicity, intermodality.

Территориальная активность (ТА) – это пространственное распределение (расположение, размещение), функционирование и взаимодействие в определенном районе или регионе (участке земной поверхности, акватории) хозяйства и социума, их инфраструктуры, органов управления, взаимодействующих и обеспечивающих структур [1, 2]. Характерными примерами МТА являются промышленное производство, энергетика, сельское хозяйство, транспорт.

Объекты ТА располагаются и функционируют на или относительно поверхности Земли (ПЗ), т.е. обладают сущностным свойством геопространственности [3].

Управление ТА как территориальной сущностью (или, по-другому геоконтроллинг, территориальное управление, геоинформационная поддержка управления) – это реализация особым специальным образом приемов и методов классического управления (целенаправленное воздействие «руководства» на «подчиненных» для достижения определенной цели) применительно к специфическим контроллинговым объектам – территориальным объектам (ТО) и структурам [4-7].

Территориальность (или геопространственность) той или иной структуры определяется [8]:

- ее положением относительно поверхности Земли (ПЗ);
- ее собственным пространством (территориальным распределением – периметр, локация);
- пространственными связями и отношениями с другими территориальными объектами или системами; особенностями ее функционирования в окружающей среде (ОС) или геосреде (ее распространение и перемещение в ОС);
- взаимовлияние ТО и ОС).

Особенность приемов и методов геоконтроллинга или территориального управления состоит в пространственной интерпретации и представлении категорий и этапов классических элементов и процедур управления (задача, обстановка, оценка обстановки, решение, план, реализация решения, ...), их перманентном отображении относительно поверхности Земли (ПЗ), генерировании территориальных рекомендаций по локализации (аллокации) района действий подчиненных структур и способам решения стоящих задач [9, 10].

Таким образом, геоконтроллинг или территориальное управление (ТУ) – это управление территориально распределенными пространственными объектами, системами и процессами, которое [11, 12]:

- 1) базируется на известных базовых подходах теории управления социальными и организационно-техническими системами;
- 2) имеет свои специфические геоконтроллинговые принципы: геосистемности – совместная обработка различных форм представления и видов геоинформации (ГИ) – априорной, оперативной, статической, динамической, медийной, графической, описательной, топологической и т.д.; хорологизации – пространственное представление категорий, процессов и этапов управления; топологизации ГИ – уход от географической конкретики в пространство рекомендаций; активности ГИ – переход от карты-подложки к геоизображению-рекомендации и др.;
- 3) подразумевает постоянное использование больших объемов разнородной разноуровневой разномасштабной динамической ГИ – информации, имеющей привязку к поверхности Земли (ПЗ);



4) имеет свои особенности, связанные со спецификой пространственной локализации и функционирования территориальных объектов, систем и процессов.

Геоконтроллинг (ГК) тождественен понятию «автоматизированное управление» применительно к особым, а именно территориальным объектам и процессам. Он реализуется посредством классических процедур (этапов) управления:

- уяснение или генерация задачи;
- формирование и ведение обстановки (сбор, обработка, отображение информации об обстановке);
- оценка обстановки в соответствии с решаемой задачей;
- выработка рекомендаций;
- планирование (если необходимо);
- организация реализации принятого решения.

Отличие ГК от автоматизированного управления территорией – это сплошная сквозная непрерывная пространственная интерпретация этапов и категорий (задача, оценка, решение, план, команда) управления. Т.е. целиком и полностью «воюем» на карте (геоизображении (ГИз)). Хотя карта здесь выступает не просто технической подложкой-носителем геоинформации (ГИ), а является активным субъектом управления – генерирует и показывает в геопространстве (ГП) где и как надо действовать.

ГК реализуется через систему геоконтроллинговых принципов и требований, к числу которых относятся: киберспособность системы управления территорией, активность карты, хорологизация, топологизация, геосистемность, интермодальность и др.

Основной принцип ГИУ требует киберспособности системы управления ТА, сквозной непрерывной обработки многоуровневой разнородной ГИ на всех этапах и во всех процедурах управления ТО. При этом форма представления данных обстановки должна соответствовать ее пространственному содержанию, а пассивная карта-подложка, служащая для нанесения обстановки, должна трансформироваться в активное геоизображение, показывающее, где и как может (или должен) действовать территориальный объект.

Киберспособность – это наличие в системе ТА и ее органе управления необходимой априорной и оперативной информации об обстановке, адаптированной цифровой базы (депозитария) рекомендаций (руководящих документов), своевременное полное точное обеспечение органа управления (ЛПР) ситуационной и координатной информацией, устойчивой связью и телекоммуникацией.

Киберспособность – это необходимое условия для построения системы ГК территорией. Это требование носит по отношению ко множеству принципов ГИУ надсистемный характер, т. к. вне этого качества для геоконтроллинга недоступны сервисы получения оперативных данных обстановки от глобальной системы наблюдения, координатной информации, запрашиваемых режимных геоданных, корректурной картографической, навигационно-гидрографической и гидрометеорологической информации. Что в свою очередь «обнуляет» требования актуализации, геосистемности и интермодальности процессов обработки и использования ГИ.

Частные геоконтроллинговые принципы – это специальные требования по представлению и использованию ГИ в органах управления ТА. Сюда входят следующие принципы представления и использования пространственной информации при управлении ТО, ТС и ТП:

- хорологизации;
- топологизации;
- анаморфирования;
- актуализации;
- геоактивности;
- интермодальности;
- геосистемности.

Хорологизация – это территориально-пространственная интерпретация и представление всех категорий и этапов управления в картографической форме (или в виде геоизображения). Все представляемые в обычном управлении в описательной и графической форме этапы и категории управления (задача, обстановка, решение, план, геокомандная технология) должны картографически интерпретироваться и содержательно отображаться в соответствующих геомоделях, базах данных, на электронной карте (ЭК) или ГИз.

Топологизация – противоположность хорологизации. Это отход от географической конкретики реальной геоситуации и переход в некую графическую абстракцию, имеющую гомоморфную связь с исходной территорией. Такой подход обеспечивает связь реальной географической обстановки с абстрактным пространством рекомендаций. Таким образом обеспечивается возможность поиска в множестве (базе, пространстве) абстрактных рекомендаций (руководящие документы) подходящего для конкретной геоситуации аналога или прототипа решения в типовой «тактической» ситуации.

Анаморфирование – это принудительное искажение картографической проекции для территориального выделения на исходной карте (или ГИз) интересующих зон при сохранении общей ситуации в искаженной «географии» [13, 14]. Реализуется за счет введения в уравнение картографической проекции анализируемого территориального параметра. Обеспечивает возможность детализации обстановки в интересующем районе за счет локального увеличения масштаба ГИз. Служит одним из инструментов территориального анализа. Может

выступать в качестве процедуры оценки обстановки. При анаморфировании полностью сохраняется пространственная топология реальной ситуации.

Актуализация – автоматическое поддержание обрабатываемой ситуационной ГИ на уровне современности. Как по содержанию, так и по расположению в геопространстве. Геоактивность – переход от пассивной карты-подложки (только носитель ГИ) к активному геоизображению, обеспечивающему генерирование и показ рекомендуемого места (где действовать) и характера (содержания) действий в указанной геолокации (как действовать).

Интермодальность – организация совместной обработки информации различных форм, качеств и свойств: априорной и оперативной, графической и текстовой, статической и динамической, обобщенной и детальной, реальной и идеальной, картографической и слаботорпологизированной.

Геосистемность – взаимосвязанное представление в геопространстве природы и социума, инфраструктуры и хозяйственных процессов, макро- и микроуровневой управления.

Геоконтрольные принципы связаны и взаимодействуют между собой. Так качество (принцип) актуальности ГИ (поддержание обрабатываемой ГИ на уровне современности) обеспечивает реализацию требований интермодальности, геосистемности, геоактивности. Принцип хорологизации обеспечивается аппаратом интермодальности, геосистемности. Топологизация обеспечивается свойствами анаморфирования и геосистемности. Качества хорологизации и топологизации взаимодействуют при поиске прототипа решения в множестве рекомендаций. Выбранные абстрактные варианты решений детопологизируются с помощью процедур хорологизации (или детопологизации). Все частные принципы работают на обеспечение свойства геоактивности. Описанная система геоконтрольных принципов составляет суть подхода к организации территориального управления территориальной деятельностью. Их последовательная реализация обеспечит необходимые и достаточные условия построения полнофункциональной системы территориального управления ТА.

### СПИСОК ЛИТЕРАТУРЫ

1. Бородин Е.Л., Звездарёв Д.В., Биденко С.И., Миронов А.Ю. Геоконтролинг территориальной активности на базе беспилотных летательных киберплатформ // Эксплуатация морского транспорта. – 2024. - № 4. – С. 54 – 61.
2. Введение в геоинформационное управление. Учебное пособие // Вагизов М.Р., Истомин Е.П., Колбина О.Н., Присяжнюк С.П., Соколов А.Г., Яготинцева Н.В. СПб.: НП «БИУ», 2021. - 352 с.
3. Геоинформационное управление развитием природно-технических систем / Истомин Е.П., Присяжнюк С.П., Соколов А.Г. и др. – СПб.: Свое издательство, 2022. – 419 с.
4. Груздев В. М. Территориальное планирование. Теоретические аспекты и методология пространственной организации территории – Н. Новгород: ННГАСУ, 2014. - 146 с.
5. Звездарёв Д.В., Биденко С.И., Доценко С.М. Геомоделирование транспортной системы в аспекте ее территориальных, ситуационных и рискологических дискурсов // Информация и Космос. – 2024. - № 2. – С. 152 – 162.
6. Зубков Ю.С. Становление и сущность геоинформационного подхода к территориальному управлению // Информатика и вычислительная техника. – 1994. - №1. – с. 11-15.
7. Истомин Е.П., Соколов А.Г. Управленческие решения. Учебник. СПб: ООО «Андреевский издательский дом», 2011 г. - 314 стр.
8. Панамарев Г.Е., Биденко С.И. Геоинформационная поддержка управления сложными территориальными объектами и системами: Монография. – Новороссийск: Изд-во ГМУ, 2012. – 202 С.
9. Стратегическое управления территориями / учебник, в 2 частях /Соколов А.Г., Истомин Е.П. и др., под. ред. Михеева В.Л. - СПб.: ООО «Андреевский изд. дом», 2018. -. 1025 с.
10. Технологии построения когнитивных транспортных систем. – СПб.: ИИТ РАН, 2018. – 268 с.
11. Якушев Д.И., Биденко С.И. Геоинформационные управляющие системы и технологии: Монография. – СПб.: Изд-во СПбУ МВД России, 2014. – 248 с.
12. Звездарёв Д.В., Биденко С.И. и др. Геоконтролинг и моделирование рисков территориальной активности / под ред. проф. С. И. Биденко: Монография – СПб.: Изд-во СПбГЭТУ «ЛЭТИ». – 2025. – 263 с.
13. Гусейн-Заде С.М., Тикуннов В.С. Анаморфозы: что это такое? - М.: Эдиториал УРСС, 1999. – 168 с.
14. Суворов А.К. Топология и преобразование картографических изображений // Геодезия и картография. 1984. № 12. С. 28-31.

УДК 621.396.4

### **ОСОБЕННОСТИ ФУНКЦИОНИРОВАНИЯ И УСЛОВИЯ ПРИМЕНЕНИЯ СРЕДСТВ ДОВЕРЕННОЙ ЗАГРУЗКИ УРОВНЯ БАЗОВОЙ СИСТЕМЫ ВВОДА-ВЫВОДА НА АВТОМАТИЗИРОВАННЫХ РАБОЧИХ МЕСТАХ ПОЛЬЗОВАТЕЛЕЙ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ И ТЕХНОЛОГИЙ**

**Виноградов Владислав Романович, Парашук Игорь Борисович**

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр-т, д. 3, Санкт-Петербург, 194064, Россия

e-mails: vladislavvinogradov4165@gmail.com, shchuk@rambler.ru

**Аннотация.** Рассмотрены ключевые понятия, связанные с определением сущности и применением средств доверенной загрузки уровня базовой системы ввода-вывода. Исследованы, проанализированы и систематизированы особенности функционирования и условия применения средств доверенной загрузки уровня базовой системы ввода-вывода на автоматизированных рабочих местах пользователей телекоммуникационных сетей и технологий. Предполагается, что это позволит систематизировать, классифицировать и учесть все влияющие на данные программно-аппаратные устройства факторы, позволит обоснованно подойти к решению важной задачи рационального выбора недорогих, но эффективных средств борьбы с несанкционированным доступом такого класса.

**Ключевые слова:** средство доверенной загрузки; базовая система ввода-вывода; телекоммуникационная сеть; автоматизированное рабочее место; рациональный выбор.

## FUNCTIONING FEATURES AND CONDITIONS OF USE OF TRUSTED LOADING TOOLS OF THE BASIC INPUT-OUTPUT SYSTEM LEVEL AT AUTOMATED WORKPLACES OF USERS OF TELECOMMUNICATION NETWORKS AND TECHNOLOGIES

**Vinogradov Vladislav, Parashchuk Igor**

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny,  
3 Tikhoretsky Av, St. Petersburg, 194064, Russia  
e-mails: vladislavvinogradov4165@gmail.com, shchuk@rambler.ru

**Abstract.** The key concepts related to the definition of the essence and application of trusted boot tools of the basic input-output system level are considered. The features of functioning and conditions of application of trusted boot tools of the basic input-output system level at automated workstations of users of telecommunication networks and technologies are investigated, analyzed and systematized. It is assumed that this will allow to systematize, classify and take into account all factors affecting these software and hardware devices, will allow to reasonably approach the solution of the important problem of rational selection of inexpensive but effective means of combating unauthorized access of this class.

**Keywords:** trusted boot facility; basic input-output system; telecommunications network; automated workstation; rational choice.

Состоявшийся переход на новый этап эволюции в области телекоммуникационных сетей и технологий (ТКСиТ), обусловил объективную необходимость внедрения в повседневную жизнь пользователей этих сетей и технологий стойкой системы защиты автоматизированных рабочих мест (АРМ), ибо утрата информации может дорого обойтись как человеку, так и государству. Именно поэтому вопросы совершенствования средств доверенной загрузки (СрДЗ) затрагивают как национальные, государственные организации нашей страны, так и интересы конкретных частных пользователей ТКСиТ. Обладая конфиденциальной информацией или информацией, содержащей сведения, составляющие коммерческую или государственную тайну, пользователи вынуждены обеспечивать надежную защиту своих АРМ от несанкционированного доступа (НСД), обеспечивать конфиденциальность, целостность и доступность информации [1–4].

В этой связи особую значимость приобретают СрДЗ, обеспечивающие специальную пошаговую проверку целостности аппаратно-программных средств АРМ пользователей ТКСиТ, а также аппаратную идентификацию и персональную аутентификацию самих пользователей на объектах и функциональных элементах сетей и систем. Подразумевается, что СрДЗ реализуют функции персонального АРМ, нацеленные на блокирование его несанкционированного запуска пользователем ТКСиТ, на препятствование загрузке операционной системы и на запрет получения возможности доступа неассоциированного с ТКСиТ пользователя к служебной информации [4–6].

Современные СрДЗ, часто называемые аппаратно-программными модулями доверенной загрузки, представляют собой комплексы аппаратно-программных механизмов, устройств или блоков, устанавливаемых (встраиваемых) в АРМ пользователей ТКСиТ и гарантирующих качественный текущий контроль доступа пользователя к этому рабочему месту, а также контроль целостности его программной среды. Существуют различные уровни реализации доверенной загрузки, но, на наш взгляд, особую актуальность на современном этапе приобрели средства доверенной загрузки уровня базовой системы ввода-вывода (БСВВ). Под БСВВ традиционно понимается набор низкоуровневых программ, загруженных в специальный чип на материнской плате АРМ и предназначенный для первоначального запуска компьютера АРМ, настройки оборудования и обеспечения функций ввода-вывода, т.е. БСВВ предоставляет набор инструкций и отвечает за загрузку компьютера АРМ пользователя ТКСиТ.

Средства доверенной загрузки уровня БСВВ, это современные программно-технические средства, которые встраиваются в базовую систему ввода-вывода и осуществляют блокирование попыток несанкционированной загрузки нештатной операционной системы, но не препятствует доступу к информационным ресурсам в случае успешных контроля целостности своего программного обеспечения и среды функционирования, проверке подлинности пользователя и загружаемой операционной системы [4, 7].

К особенностям функционирования СрДЗ уровня БСВВ на АРМ пользователей ТКСиТ относят тот факт, что данные средства функционально встраиваются в базовую систему ввода-вывода и гарантируют невозможность подключения нарушителя «в разрыв» между базовой системой ввода-вывода АРМ пользователя и самим СрДЗ. При этом выполняется ряд процедур, ярко характеризующих современные условия применения СрДЗ уровня БСВВ на АРМ пользователей ТКСиТ: самопроверка (самотестирование) СрДЗ; получение управления в процессе выполнения БСВВ до передачи управления для загрузки операционной системы (ОС) АРМ пользователя ТКСиТ с машинного носителя информации; идентификация и аутентификация пользователя ТКСиТ с использованием портов ввода-вывода его АРМ; контроль целостности среды функционирования (программной среды и элементов аппаратного обеспечения АРМ пользователей ТКСиТ); продолжение выполнения БСВВ с последующей загрузкой ОС в случае положительной аутентификации пользователя АРМ ТКСиТ; блокировка загрузки АРМ пользователя ТКСиТ в случае превышения допустимого количества неудачных попыток аутентификации этого пользователя или попытки загрузки нештатной ОС; регистрация событий безопасности и запись информации аудита в выделенную область памяти [7].

Рассмотренные условия применения СрДЗ уровня БСВВ на АРМ пользователей ТКСиТ обуславливают их функциональные возможности, к которым можно отнести: возможность регистрации возникновения событий, относящихся к безопасности и контролируемых СрДЗ; возможность реагирования на обнаружение событий, указывающих на возможное нарушение безопасности; возможность контроля целостности загружаемой ОС; возможность со стороны администраторов СрДЗ управлять режимом выполнения функций безопасности данного средства; возможность со стороны администраторов СрДЗ управлять данными (данными СрДЗ), используемыми функциями безопасности СрДЗ; поддержку определенных ролей (учетных записей пользователей) для СрДЗ и их ассоциации с конкретными администраторами СрДЗ и пользователями ТКСиТ; возможность тестирования (самотестирования) функций безопасности СрДЗ, проверки целостности программного обеспечения СрДЗ и целостности данных СрДЗ; блокирование загрузки ОС при выявлении попыток загрузки нештатной ОС; блокирование загрузки операционной системы при превышении числа неудачных попыток аутентификации пользователя; блокирование загрузки операционной системы при нарушении целостности СрДЗ; блокирование загрузки ОС при нарушении целостности загружаемой программной среды; блокирование загрузки ОС АРМ при критичных типах сбоев и ошибок [4, 7].

Важной проблемой является рациональный выбор недорогих, но эффективных СрДЗ уровня БСВВ на АРМ пользователей ТКСиТ. Рациональный выбор СрДЗ уровня БСВВ должен быть основан на строгих математических, алгоритмических и методологических правилах (механизмах) селекции подобных устройств, которые позволят наиболее полно учитывать их свойства, позволят подстраивать характеристики процедур выбора СрДЗ в соответствии с изменяющимися задачами обеспечения принципов и регламентов политики безопасности, с учетом степени наблюдаемости параметров СрДЗ и характера неопределенности измеряемых (моделируемых) данных наблюдения и исследования вариантов и условий их применения.

Таким образом, рассмотренные и проанализированные особенности функционирования и условия применения средств доверенной загрузки уровня базовой системы ввода-вывода на автоматизированных рабочих местах пользователей телекоммуникационных сетей и технологий позволяют систематизировать, классифицировать и учесть все влияющие на данные программно-аппаратные устройства факторы, позволяют обоснованно подойти к решению важной задачи рационального выбора недорогих, но эффективных средств борьбы с НСД такого класса. Результаты анализа особенностей работы и условий применения СрДЗ уровня БСВВ являются, по сути, исходными данными для разработки специальных методов и алгоритмов рационального выбора подобных устройств, что в конечном итоге, призвано повысить эффективность их применения в реальной динамике предотвращения несанкционированного доступа.

#### СПИСОК ЛИТЕРАТУРЫ

1. Аvezова Я.Э., Фадин А.А. Вопросы обеспечения доверенной загрузки в физических и виртуальных средах // Вопросы кибербезопасности. №1(14). 2016. С. 24-30.
2. Модестов А.А., Беляева Е.А. Комплексная оценка функциональных возможностей аппаратно-программных модулей доверенной загрузки // Вестник Российского нового университета. 2013 № 4 С. 105-107.
3. Левенков О.А. Средства доверенной загрузки // Технологии безопасности. 2013. № 6. С. 40-41.
4. Жмуров В.Д., Парашук И.Б., Саяркин Л.А. Типы средств доверенной загрузки и их роль в обеспечении информационной безопасности телекоммуникационных сетей // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 4. СПОИСУ. СПб.: 2017. С. 82-84.
5. Парашук И.Б., Крюкова Е.С., Саяркин Л.А., Малофеев В.А. Обзор и анализ показателей качества современных средств доверенной загрузки автоматизированных рабочих мест, подключаемых к электронным библиотекам // Science And Educations: Problems And Innovations: Сборник статей IV Международной научно-практической конференции. Пенза: Наука и Просвещение. 2020. С. 76-78.
6. Парашук И.Б., Башкирцев А.С., Саяркин Л.А. Вариант формулировки показателей качества современных средств доверенной загрузки и их роль при решении проблем безопасности алгоритмов управления инфотелекоммуникационными системами специального назначения // Вопросы оборонной техники. Научно-технический журнал. Серия 16. 2016. №5-6. С. 47-51.
7. Методический документ. Профиль защиты средства доверенной загрузки уровня базовой системы ввода-вывода. Четвертый класс защиты. ИТ.СДЗ.УБ4.ПЗ. М.: ФСТЭК России. 2013. 52 с.

УДК 004.94

#### МОДЕЛИРОВАНИЕ СОСТОЯНИЯ ВНЕШНЕЙ СРЕДЫ С ВЫЯВЛЕНИЕМ ТЕРРИТОРИЙ ОПАСНЫХ АТМОСФЕРНЫХ И ТЕХНОГЕННЫХ ВОЗДЕЙСТВИЙ

Глушченко Артём Геннадьевич

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)  
Профессора Попова ул., 5, Санкт-Петербург, 197022, Россия  
e-mail: agglushchenko@etu.ru

**Аннотация.** Для моделирования состояния внешней среды с выявлением территорий опасных атмосферных и техногенных воздействий рассмотрены возможности моделей информационного описания состояния внешней среды, отражающих влияние различных типов воздействий на них: атмосферных условий, переменных атмосферных и техногенных воздействий. Выделены преимущества моделей во взаимосвязи с перечнем факторов, данные по которым эти модели используют для параметрического описания и вычислений. Контроль и прогнозирование состояния внешней среды позволит описать состояния безопасности, напряженности, загрязнённости и опасности внешней среды.

**Ключевые слова:** безопасные информационные системы; моделирование информационной системы; моделирование состояния внешней среды; прогнозирование состояния моделируемой информационной системы.

## MODELING THE STATE OF THE EXTERNAL ENVIRONMENT WITH IDENTIFICATION OF TERRITORIES OF DANGEROUS ATMOSPHERIC AND TECHNOGENIC IMPACTS

Glushchenko Artem

Saint Petersburg Electrotechnical University  
5 Professora Popova St, St. Petersburg, 197022, Russia  
e-mail: agglushchenko@etu.ru

**Abstract.** The possibilities of models of information description of the state of the external environment, reflecting the influence of various types of impacts on them: atmospheric conditions, variable atmospheric and technogenic impacts, are considered. The advantages of models in relation to the list of factors, data on which these models use for parametric description and calculations, are highlighted. Monitoring and forecasting the state of the external environment will allow describing the states of safety, tension, pollution, and danger of the external environment.

**Keywords:** secure information systems; modeling of an information system; modeling of the external environment; forecasting the state of the modeled information system.

К предметной области информационной безопасности транспортных систем можно отнести информационную поддержку состояния внешней среды и учёт возможного воздействия на них атмосферных условий и переменных атмосферных и техногенных воздействий. Наравне с использованием известных моделей [1–3], отражающих влияние различных типов воздействий на окружающую среду, перспективной задачей является построение модели, сочетающей факторы, учитываемые в традиционных апробированных моделях [1–3]. Были проанализированы модели, связанные с загрязнением атмосферы отходами и продуктами производства и потребления; технологическими загрязнениями, возникающими при производстве или транспортировке; сопутствующими потерями при технологических особенностях производственного цикла или транспортировке применяемого сырья ряда физико-химических составов. Моделирование состояний объекта (как информационной системы) и характера воздействия на него внешней среды, атмосферных условий, переменных атмосферных и техногенных факторов позволит контролировать состояние безопасности моделируемой информационной системы.

Контроль и прогнозирование состояния внешней среды от подобных воздействий и загрязнений является предметом информационного описания как в статике, так и динамике развития загрязнения и атмосферного воздействия. Современные модели описания состояния внешней среды в значительной степени базируются на достижениях в области машинного обучения для рекомендательных систем и искусственного интеллекта [4]. Широкие вычислительные возможности средств формирования массивов данных, включая «большие данные», проблемно-ориентированные коллекции данных для различных прикладных областей, возможность сопряжения с сервисными и тематическими библиотеками, позволяют обеспечить описание самого объекта контроля, динамику его состояний, состояния условий окружающей среды и динамику состояний объекта в условиях динамики условий окружающей среды.

Анализ вычислительных возможностей и специфики описаний объектов моделей [1–3] и схожих с ними позволил выявить преимущества выделенных моделей во взаимосвязи с перечнем факторов, данные по которым эти модели используют для параметрического описания и вычислений.

В модели «Гаусс», учитывающей предсказания диффузии воздушно-распространяемых загрязнителей, загрязнение описано нормальным распределением и распределяется в соответствии с законом Фика, в параметрах модели учитываются факторы химического состояния загрязняющего вещества и параметры состояния окружающей среды: скорость и направление ветра, характер атмосферных возмущений, расположение источника загрязнений тенденции его поведения в зависимости от физических свойств загрязнителя.

В модели «ИЭС» (информационно-энергетическая система), основанной на методе Эйлера захвата, учитывается динамика загрязнения в конечном объеме атмосферы, параметрически описываются факторы смещения веществ, тенденции к выпадению и оседанию, возможно возникающие химические реакции среды с взаимодействующими веществами. Модель учитывает нестационарные условия изменения скорости и направления ветра, цикличность и периодичность воздействия источника загрязнения. Удобство использования модели «ИЭС» подтверждается её применимостью в оценке состояния экосистем и промышленных экосистем [5, 6].

Модель «Пуфф» применяется для оценки распространения веществ в сочетании с моделью диффузии, модель позволяет отобразить перемещение источника загрязнения под воздействием атмосферных потоков. Модель учитывает факторы: высота источника загрязнения, интенсивность выброса, скорость и направление ветра, турбулентность и другие переменные атмосферные условия.

Распространенной моделью для оценки распространения загрязняющих веществ является модель «Сетчатка». В этой модели загрязнение распределяется на пространственную сетку с использованием уравнений диффузии или конвекции, что позволяет более точно предсказывать распространение из-за более подробного разбиения на сектора изучаемой области. В сочетании с графическими моделями масштабирования Миллера можно наглядно отобразить зону загрязнения (потенциального загрязнения, степеней потенциального загрязнения) или зону воздействия атмосферного влияния (потенциального возмущения, степеней потенциального возмущения окружающей среды).

Таким образом, существует несколько моделей оценки распространения загрязняющих веществ и напряженных атмосферных воздействий, каждая из которых основывается на различных предположениях и методах. Проведено моделирование на контрольных примерах для всех описанных моделей, выявлены их особенности, преимущества и ограничения. Сделан вывод, что точный выбор базовой модели для разработки модели целевого назначения может обосновываться параметрической базой описания или системы реагирования на состояния модели, вида загрязняющих веществ, типичных или специфичных условий окружающей среды, что обеспечит более точные прогнозы и поможет принять более эффективные меры по обеспечению безопасности. Рассмотрены блоки обязательных параметров описания для решения конкретных задач моделирования состояния внешней среды и выявления на контролируемой территории опасных проявлений атмосферных и техногенных воздействий.

#### СПИСОК ЛИТЕРАТУРЫ

1. Rolph G.D., F. Ngan, R.R. Draxler. Modeling the fallout from stabilized nuclear clouds using the HYSPLIT atmospheric dispersion model. *Journal of Environmental Radioactivity*, pp. 41-55, 2014.
2. Pei Z., L. Zube. Impacts of wind speed and leakage height on chlorine leakage diffusion. 2014 International Symposium on Safety Science and Technology. 2014. pp. 672-681.
3. Huimin L., Z. Xuezhi, C. Haiping, H. Shunxiang, L. Feng, W. Gang. Numerical Simulation and Field Experiment Validation of Atmospheric Pollution Chemical Accidents Based on Canopy Model. 2011 International Conference on Environmental Science and Engineering. 2012. pp.30-37.
4. Elsevier B.V. Unveiling the Latest Trends and Advancements in Machine Learning Algorithms for Recommender Systems: A Literature Review. 11th CIRP Global Web Conference (CIRPe 2023). 2024. pp. 115-120.
5. Чихонадских Е.А., Черкаев Г.В. Управление природопользованием: учебник. СПб. СПбГМТУ, 2013. 204 с.
6. Черкаев Г.В. Математическое моделирование рассеивания загрязняющих веществ от судостроительного предприятия в атмосфере // Морские интеллектуальные технологии. 2019. Т. 1. Вып. 2 (44) С. 197-202.

УДК 004.89

#### ГЕНЕРАТИВНЫЙ ПОДХОД К СОЗДАНИЮ АНОНИМИЗИРОВАННЫХ ЦИФРОВЫХ ДВОЙНИКОВ ТЕЛЕКОММУНИКАЦИОННЫХ БИЗНЕС-ПРОЦЕССОВ В ФОРМАТЕ ГРАФА ЗНАНИЙ

Головин Алексей Андреевич<sup>1</sup>, Жукова Наталия Александровна<sup>2</sup>

<sup>1</sup>Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Профессора Попова ул., 5, Санкт-Петербург, 197022, Россия

<sup>2</sup>СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия

e-mails: golovin99@icloud.com, nazhukova@mail.ru

**Аннотация.** В данной работе представлен генеративный подход к созданию анонимизированных цифровых двойников телекоммуникационных бизнес-процессов на основе графов знаний. Предложенная методология использует эталонную модель TM Forum Framework (TMF) в качестве базиса для генерации синтетических наборов данных с применением больших языковых моделей для обеспечения структурной вариативности и семантической согласованности. Разработанный подход позволяет создавать реалистичные модели бизнес-процессов, сохраняя конфиденциальность исходных данных организации.

**Ключевые слова:** графы знаний; цифровые двойники; телекоммуникационные системы; генерация синтетических данных; TM Forum; большие языковые модели.

#### GENERATIVE APPROACH TO CREATING ANONYMIZED DIGITAL TWINS OF TELECOMMUNICATION BUSINESS PROCESSES IN THE FORMAT OF A KNOWLEDGE GRAPH

Golovin Aleksei<sup>1</sup>, Zhukova Nataly<sup>2</sup>

<sup>1</sup> St. Petersburg State Electrotechnical University «LETI»

5 Professor Popov St, St. Petersburg, 197022, Russia

<sup>2</sup> St. Petersburg Federal Research Center of the Russian Academy of Sciences

39 14th Line VO, St. Petersburg, 199178, Russia

e-mails: golovin99@icloud.com, nazhukova@mail.ru

**Abstract.** This paper presents a generative approach to creating anonymized digital twins of telecommunication business processes based on knowledge graphs. The proposed methodology uses the TM Forum Framework (TMF) reference model as a basis for generating synthetic datasets using large language models to ensure structural variability and semantic consistency. The developed approach allows creating realistic business process models while maintaining the confidentiality of the organization's original data.

**Keywords:** knowledge graphs; digital twins; telecommunication systems; synthetic data generation; TM Forum; large language models.

Современные телекоммуникационные компании сталкиваются с растущей потребностью в цифровой трансформации бизнес-процессов и создании их цифровых двойников для оптимизации операционной деятельности [1]. Однако использование реальных данных организаций для разработки и тестирования аналитических систем часто ограничено требованиями конфиденциальности и информационной безопасности.

Решением данной проблемы является применение синтетических наборов данных, которые воспроизводят ключевые характеристики реальных бизнес-процессов без раскрытия чувствительной информации [2].

Графы знаний представляют собой эффективный инструмент для моделирования сложных взаимосвязей в телекоммуникационном домене, позволяя представить бизнес-процессы, сервисы, ресурсы и их взаимодействия в виде структурированной семантической сети [3]. Эталонная модель TM Forum Framework (TMF) является де-факто стандартом в индустрии телекоммуникаций, предоставляя унифицированную архитектуру бизнес-процессов, информационную модель и интерфейсы приложений [4].

В данной работе предлагается генеративный подход к созданию синтетических цифровых двойников телекоммуникационных бизнес-процессов, основанный на использовании модели TMF в качестве эталонного шаблона. Ключевой особенностью подхода является введение контролируемой структурной вариативности для моделирования реальных отклонений от эталонной модели, характерных для конкретных организаций.

Предложенная методология начинается с базовой генерации структуры графа знаний на основе TMF. Исходная структура формируется с использованием компонентов модели TMF, включая eTOM (enhanced Telecom Operations Map) для бизнес-процессов, SID (Shared Information/Data model) для информационной модели и TAM (Telecom Application Map) для приложений. Такой подход обеспечивает соответствие генерируемых данных отраслевым стандартам и создает прочную основу для дальнейших модификаций.

Следующим важным этапом является введение структурной вариативности для приближения синтетических данных к реальным организационным структурам. На этом этапе в граф знаний вносятся нетиповые взаимосвязи и вариации структурных паттернов. Процесс включает добавление дополнительных сущностей, отражающих специфические бизнес-процессы конкретной организации, модификацию существующих связей для представления альтернативных процессных маршрутов, исключение неиспользуемых компонентов эталонной модели и создание кросс-функциональных связей между различными доменами. Такой подход позволяет моделировать реальное разнообразие телекоммуникационных систем, сохраняя при этом структурную целостность.

Особое внимание в предложенной методологии уделяется семантическому обогащению с использованием больших языковых моделей (LLM). Применение LLM обеспечивает генерацию контекстно-зависимых описаний и атрибутов сущностей, что критически важно для создания реалистичных синтетических данных [5]. Языковые модели создают уникальные наименования и описания для новых сущностей, выполняют перефразирование стандартных описаний TMF с сохранением их семантического значения, генерируют реалистичные значения атрибутов на основе контекста телекоммуникационного домена и обеспечивают терминологическую согласованность в рамках всего графа знаний. Это позволяет создавать синтетические данные, которые не только структурно корректны, но и семантически осмысленны.

Контроль качества и валидация генерируемых графов знаний представляют собой многоуровневый процесс проверки. На первом уровне выполняется структурная валидация на соответствие ограничениям целостности, затем проводится семантическая проверка на логическую согласованность связей между сущностями. Завершающим этапом является оценка реалистичности через сравнение со статистическими характеристиками реальных телекоммуникационных систем. Такой комплексный подход к валидации гарантирует высокое качество генерируемых синтетических данных.

Архитектура предложенного решения представляет собой модульную систему, включающую модуль парсинга эталонной модели TMF, генератор структурных вариаций, семантический процессор на основе LLM и модуль экспорта в различные форматы графов знаний, такие как RDF и Property Graph. Управление процессом генерации осуществляется через конфигурационные параметры, которые определяют степень отклонения от эталонной модели, типы вводимых вариаций и требуемый уровень детализации. Такая архитектура обеспечивает гибкость и масштабируемость решения.

Основными преимуществами предложенного подхода являются сохранение отраслевой специфики за счет использования модели TMF, гибкая настройка уровня вариативности и сложности генерируемых структур, автоматическое обеспечение семантической согласованности через применение LLM, масштабируемость для создания графов различного размера и возможность генерации множественных вариантов для тестирования устойчивости аналитических систем. Эти преимущества делают подход универсальным инструментом для различных задач в телекоммуникационном домене.

Применение генерируемых синтетических цифровых двойников охватывает широкий спектр сценариев. Среди основных областей применения можно выделить разработку и тестирование систем искусственного интеллекта для телекоммуникационного домена, обучение персонала без риска воздействия на производственные системы, проведение исследований в области оптимизации бизнес-процессов и бенчмаркинг алгоритмов обработки графов знаний [6]. Синтетические данные позволяют проводить эксперименты и исследования, которые были бы невозможны или крайне рискованны на реальных системах.

Таким образом, в данной работе представлен комплексный подход к генерации анонимизированных цифровых двойников телекоммуникационных бизнес-процессов в формате графа знаний. Использование эталонной модели TMF в сочетании с контролируемой вариативностью и семантическим обогащением через LLM позволяет создавать реалистичные синтетические наборы данных, пригодные для широкого спектра исследовательских и практических задач при соблюдении требований информационной безопасности.

## СПИСОК ЛИТЕРАТУРЫ

1. Westerlund M., Isabelle M., Leminen S. The acceptance of digital surveillance in an age of big data // *Technology Innovation Management Review*. Vol. 11, 2021, № 3. P. 32-44.
2. Nikolenko S. I. Synthetic data for deep learning // *Springer Optimization and Its Applications*. Vol. 174, 2021. P. 1-195.
3. Auer S., Oelen A., Haris M., Stocker M., D'Souza J., Farfar K. E., Vogt L., Prinz M., Wiens V., Jaradeh M. Y. Open Research Knowledge Graph: A System for Managing Large-Scale Neuro-Symbolic Knowledge // *Handbook on Neurosymbolic Artificial Intelligence and Knowledge Graphs*. IOS Press, 2025. P. 385-420.
4. TM Forum. Business Process Framework (eTOM) // TM Forum Technical Specification. 2025.
5. Yao L., Mao J., Luo Y., Zhang Y., Zhang Y., Liu K., Zhao J. Exploring Large Language Models for Knowledge Graph Completion // *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2025. P. 1-5. Dettmers T., Minervini P., Stenetorp P., Riedel S. Convolutional 2d knowledge graph embeddings // *Proceedings of the AAAI Conference on Artificial Intelligence*. Vol. 32, 2018, № 1, P. 1811-1818.
6. Venkatakrishnan V. N. Real-time Analytics for APT Detection and Threat Hunting Using Cyber-threat Intelligence and Provenance Graphs // *Proceedings of the 2025 ACM International Workshop on Security and Privacy Analytics*. 2025. P. 1-1.

УДК 004.7

**СОВРЕМЕННЫЙ ПОДХОД К ПОСТРОЕНИЮ ПРОГРАММНО-ОПРЕДЕЛЯЕМЫХ  
БЕСПРОВОДНЫХ СЕТЕЙ СВЯЗИ****Гордеев Михаил Алексеевич, Олимпиев Алексей Александрович**

ООО «А-риал»

Лиговский пр., 176/178, Санкт-Петербург, 192007, Россия

e-mails: eugene@xfox111.net, aao\_82@mail.ru

**Аннотация.** Рассматриваются общие тенденции развития архитектуры программного обеспечения, которое используется при организации программно-определяемых WLAN сетей и сетей сотовой связи, построенных с использованием стандартов 4/5G. Приводятся результаты опыта применения облачных технологий для реализации микросервисной архитектуры и предоставления мультисервисных сетей связи, а также особенности взаимодействия сетей, построенных с использованием разных технологий связи.

**Ключевые слова:** программно-определяемые беспроводные сети связи; облачные технологии; Kubernetes; ядро сети; микросервисная архитектура.

**A MODERN APPROACH TO CONSTRUCTING SOFTWARE-DEFINED  
WIRELESS COMMUNICATION NETWORKS****Gordeev Mikhail, Oлимпиев Aleksey**

LLC «A-rial»

176/178 Ligovsky Av, St. Petersburg, 192007, Russia

e-mails: eugene@xfox111.net, aao\_82@mail.ru

**Abstract.** The article discusses general trends in the development of software architecture used in organizing software-defined WLAN networks and cellular networks built using 4/5G standards. It presents the results of experience in using cloud technologies to implement microservice architecture and provide multiservice communication networks, as well as the features of interaction between networks built using different communication technologies.

**Keywords:** software-defined wireless networks; cloud technologies; Kubernetes; kernel of network; microservice architecture.

Ни для кого не секрет, что современные системы связи работают и должны работать в соответствии с международными стандартами, благодаря чему обеспечивается сквозная совместимость сетей и оборудования любого производителя на всех уровнях модели OSI и достигается высокий уровень качества обслуживания абонентов даже в тех случаях, когда они осуществляют взаимодействие с другими абонентами, находящимися в другом конце света или в труднодоступных местах.

Эффективность развития отрасли Связь достигается за счет того, что в ней действует принцип всеобщего соблюдения действующих стандартов, а также стратегия опережающей стандартизации, в соответствии с которой международные организации могут совместно планировать развитие технологий на многие годы вперед.

В частности, организация 3GPP ведет маршрутную карту [1] развития стандартов сотовой связи и других радиосетей и регулярно выпускает обновления к ним. Так, например, на данный момент стандартизовано взаимодействие сетей 4/5G и сетей, построенных на технологии WLAN (Wifi6 и других) [2]. В то же время ведется работа над стандартизацией сетей 6G и Wifi7 с учетом особенностей постепенного перехода от оборудования и технологий предыдущего поколения к новому, которые в большей мере соответствуют растущим потребностям абонентов.

Современный подход к организации систем связи опирается на парадигму программно-определяемых сетей связи, базирующихся на использовании программно-определяемых компонентов. В беспроводных сетях связи, таких как сотовые и Wifi-сети, основными компонентами являются: программно-определяемая радиосистема, софтверный коммутатор, программно-определяемые хранилища и т. п. Данная парадигма начала развиваться еще в начале 2000-х годов и привела к концепции программно-насыщенных систем, которая позволяет создавать



программно-аппаратные комплексы любого назначения на унифицированных аппаратных компонентах за счет наполнения их необходимым прикладным программным обеспечением.

Данная парадигма архитектурно долгое время строилась на принципе ядра, включающего в себя несколько высокопроизводительных серверов и общей шины (как правило, под этим термином понималась единая распределенная база данных и унифицированный программный интерфейс к ней), к которым подключались типовые монолитные многофункциональные программные сервисы, предоставляющие механизмы для отдельных услуг связи, а в качестве центрального коммутационного узла выступал монолитный софтверный, который управлял любым мультисервисным трафиком.

Однако с появлением и развитием микросервисных и облачных архитектур, в частности программного обеспечения Kubernetes, ситуация кардинально поменялась и сейчас фактически требует переработки всех разработанных ранее программных систем, на что уйдут многие годы.

Одними из основных проблем микросервисной архитектуры являются: управляемость, сложность ее сопровождения, сложность архитектуры, информационная безопасность, недостаточная гибкость архитектуры и низкая робастность готовой системы, высокий порог вхождения и другие [3, 4].

Наиболее серьезной является проблема недостатка кодовой базы, которая вызывает доверие, достаточно дешевая, имеет долгосрочную поддержку и способна заменить существующие программные решения — те, что развивались в течение многих десятков лет. Фактически на данный момент используются те же монолиты, что и раньше, но упакованные в контейнеры — такой подход может рассматриваться, только как временное решение, которое позволит перейти к более современным технологиям.

Еще одной проблемой, которая наблюдается — дефицит специалистов, которые готовы, хотят и могут разобраться в ранее разработанном программном обеспечении, а также предложить адекватную стратегию системного перевода его на микросервисную базу.

Общий взгляд на описанные проблемы позволяет сделать вывод о том, что наиболее перспективным направлением развития IT-индустрии в будущем видится системный анализ и проектирование, которые позволят не только не потерять накопленный ведущими разработчиками опыт и знания, но и помогут развить существующие и создать новые методы рефакторинга и модернизации программного обеспечения.

#### СПИСОК ЛИТЕРАТУРЫ

1. Puneet Jain, Rel-20 Planning and Progress in TSG SA / Электронный ресурс. URL <https://www.3gpp.org/news-events/3gpp-news/sa-rel20>, (дата обращения 10.08.2025).
2. Стандарт ETSI TS 123 501 V15.2.0 (2018-06). 5G; System Architecture for the 5G System (3GPP TS 23.501 version 15.2.0 Release 15).
3. Дж. Стронг. Kubernetes и сети. Многоуровневый подход: Пер. с англ. / Дж. Стронг, В. Ленси. СПб. БВХ-Петербург, 2024. 320 с.: ил.
4. Арундел Джон, Домингус Джастин. Kubernetes для DevOps: развертывание, запуск и масштабирование в облаке. СПб.: Питер, 2020. 384 с.: ил. (Серия «Бестселлеры O'Reilly»).

УДК 621.396.4

#### ПРИМЕНЕНИЕ КВАНТОВЫХ ТЕХНОЛОГИЙ В ЦЕНТРАХ ОБРАБОТКИ ДАННЫХ

**Грибков Владимир Александрович, Михайличенко Николай Валерьевич,**

**Титов Владимир Степанович, Шарко Геннадий Васильевич**

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: 23esn2008@rambler.ru, shgorg@mail.ru, gribkov.1949@mail.ru

**Аннотация.** Разработка квантовых компьютеров открывает новые перспективы в IT, однако их потенциальное использование для кибератак требует усиления мер защиты. При этом традиционные транзисторные компьютеры сохраняют свою актуальность в большинстве сфер.

**Ключевые слова:** квантовые вычисления; кибербезопасность; центр обработки данных; кибератаки; квантовая криптография.

#### APPLICATION OF QUANTUM TECHNOLOGIES IN DATA CENTERS

**Gribkov Vladimir, Mikhailichenko Nikolay, Titov Vladimir, Sharko Gennady**

Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

(Military Academy of Telecommunications)

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: 23esn2008@rambler.ru, shgorg@mail.ru, gribkov.1949@mail.ru

**Abstract.** The development of quantum computers opens up new perspectives in IT, but their potential use for cyber-attacks requires enhanced protection measures. At the same time, traditional transistor computers remain relevant in most areas.

**Keywords:** quantum computing; cybersecurity; data center; cyberattacks; quantum cryptography.

Квантовые технологии открывают новую эпоху в сфере информационных технологий. В отличие от классических компьютеров, квантовые вычислители используют кубиты, способные существовать в

суперпозиции состояний. Это свойство обеспечивает экспоненциальное ускорение вычислений, которое можно использовать при эксплуатации центров обработки данных (ЦОД). [1, 2].

Одной из ключевых сложностей при разработке квантовых компьютеров является поддержание когерентности кубитов — минимальных единиц квантовой информации, аналогичных битам в традиционных системах. Для этого требуется исключить любые внешние помехи. Несмотря на разнообразие подходов к созданию таких устройств, большинство из них пока не готовы к массовому внедрению.

Сравнительный анализ квантовых и классических вычислительных систем демонстрирует, что квантовые компьютеры обладают значительным преимуществом в скорости при решении специализированных задач, включая факторизацию больших чисел и оптимизационные проблемы. Тем не менее, в большинстве сценариев обработки данных традиционные архитектуры сохраняют свою эффективность. Кроме того, квантовые технологии открывают новые возможности для обеспечения кибербезопасности в дата-центрах — в частности, квантовая криптография позволяет генерировать принципиально неуязвимые ключи шифрования, устойчивые к атакам классических алгоритмов.

Квантовые вычислительные системы демонстрируют значительный потенциал для ускоренного поиска информации в крупномасштабных базах данных ЦОД. Однако параллельно возникает серьезная угроза информационной безопасности: злонамеренное применение квантовых компьютеров позволяет осуществлять взлом традиционных криптографических систем. В частности, существующие алгоритмы шифрования становятся уязвимыми перед вычислительной мощностью квантовых устройств. Для противодействия этим рискам требуется разработка и внедрение квантово-устойчивых криптографических методов. Таким образом, несмотря на перспективность квантовых технологий в различных сферах (включая кибербезопасность), их широкомасштабное внедрение сдерживается необходимостью решения комплекса научно-технических задач.

Квантовые технологии знаменуют собой качественно новый этап развития IT-инфраструктуры, способный трансформировать современные системы информационной безопасности. Благодаря способности квантовых компьютеров обрабатывать колоссальные массивы данных практически мгновенно, они могут существенно усилить криптографические алгоритмы. Однако эта же технология создает серьезные риски для безопасности ЦОД, поскольку традиционные методы шифрования становятся уязвимыми перед вычислительной мощностью квантовых систем. В ответ на этот вызов специалисты по кибербезопасности разрабатывают новые защитные механизмы, устойчивые к квантовым атакам. Одним из наиболее перспективных направлений является квантовая криптография, основанная на фундаментальных принципах квантовой механики, что обеспечивает принципиально новый уровень защиты данных.

Квантовая криптография использует фундаментальные свойства квантовых систем — суперпозицию состояний и квантовую запутанность — для генерации криптографических ключей. Благодаря принципу неопределенности Гейзенберга, любая попытка перехвата ключа неизбежно изменяет его квантовое состояние, что делает вмешательство обнаружимым. Несмотря на теоретически абсолютную безопасность, практическое внедрение этой технологии сталкивается с рядом ограничений, включая высокую стоимость инфраструктуры и технические сложности реализации.

В качестве альтернативных подходов к защите от квантовых атак рассматриваются:

1. Постквантовые криптографические алгоритмы, не основанные на уязвимых к квантовым вычислениям задачах факторизации и дискретного логарифмирования.
2. Методы квантового обнаружения вторжений, отслеживающие изменения в состояниях кубитов.

Эти направления становятся особенно актуальными в контексте развития цифровой экономики и необходимости защиты данных от новых угроз [3].

Развитие квантовых технологий формирует парадоксальную ситуацию в сфере информационной безопасности: с одной стороны, они создают беспрецедентные угрозы для существующих криптографических систем, с другой — открывают возможности для разработки принципиально новых защитных механизмов. Специалистам в области кибербезопасности необходимо proactively адаптироваться к этим изменениям, непрерывно совершенствуя методы защиты данных в условиях стремительного квантового прогресса.

Потенциальные векторы квантовых кибератак включают:

- криптографические атаки с использованием квантовых алгоритмов (Шора, Гровера) для взлома традиционных ключей;
- квантовые MITM-атаки с перехватом и модификацией данных в каналах связи;
- целенаправленные атаки на квантовые сети и устройства (например, через уязвимости в QKD-системах).

При этом сохраняется риск появления новых, пока неизученных методов квантового кибервторжения, что требует разработки опережающих мер защиты.

Некоторые другие возможные способы квантовых кибератак могут включать использование квантовых алгоритмов для решения сложных математических задач, таких как поиск распределения наибольшего потока в графе или оптимизация функций. Кроме того, квантовые системы могут использоваться для создания спама, фишинга и других видов социальной инженерии. Квантовые кибератаки могут также включать в себя использование квантовых алгоритмов для взлома защиты информационных систем, а также использование квантовых технологий для создания и распространения вредоносных программ и компьютерных сетей, состоящих из некоторого количества хостов с запущенными ботами — автономным программным обеспечением.

Кроме того, квантовые кибератаки могут использовать квантовую телепортацию для передачи информации без возможности ее перехвата.

Таким образом можно провести расширенный анализ угроз квантовых кибератак.

1. Использование квантовых алгоритмов для атак на сложные системы. Квантовые компьютеры способны значительно ускорить решение оптимизационных задач, что открывает новые векторы атак:

- оптимизация атак на сети: алгоритмы квантового отжига (D-Wave) или QAOA могут использоваться для поиска уязвимых узлов в крупных сетях (например, энергосетях или финансовых системах);
- взлом защиты через машинное обучение: квантовые алгоритмы (например, квантовые нейросети) могут ускорять подбор параметров для обхода систем ИБ, основанных на AI;
- криптоанализ: алгоритм Гровера позволяет ускорить атаки на хеш-функции и симметричные шифры (AES-256 потребует в  $2^{128}$  раз меньше попыток).

2. Социальная инженерия и автоматизированные атаки:

- квантовый спам/фишинг: генеративные квантовые модели (аналоги GPT, но на квантовых схемах) могут создавать персонализированные фишинговые сообщения, анализируя Big Data жертвы за секунды;
- ботнеты с квантовым управлением: квантовые алгоритмы распределенного поиска (например, квантовые случайные блуждания) могут координировать миллионы ботов без центрального сервера, делая такие сети неотслеживаемыми.

3. Атаки на квантовую инфраструктуру:

- exploiting QKD: атаки на системы квантовой распределения ключей (например, «фазовые слепые атаки» на протокол BB84);
- квантовая телепортация для скрытого C2: Передача управляющих команд для ботнетов через запутанные состояния, что делает трафик недетектируемым классическими IDS.

4. Гибридные угрозы. Квантово-классические вирусы: вредоносное ПО, использующее квантовые подпрограммы (например, для взлома локальных ключей) в традиционных системах.

Таким образом, создание квантовых компьютеров представляет собой одно из ключевых направлений прогресса в сфере информационных технологий. Однако их потенциальное использование злоумышленниками для кибератак требует разработки новых механизмов защиты данных. В то же время, традиционные транзисторные компьютеры сохраняют свою значимость и остаются востребованными в различных областях.

#### СПИСОК ЛИТЕРАТУРЫ

1. Парашук И.Б., Чечулин А.А. Сущность и содержание задач поиска уязвимостей интерфейсов в интересах безопасного управления беспилотными транспортными средствами «умного города» // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2020). IX Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. / Под. ред. С.В. Бачевского; сост. А. Г. Владыко, Е.А. Аникевич. СПб.: СПбГУТ, 2020. Т.1. С. 759-763.
2. Национальный стандарт РФ ГОСТ Р 52633.4-2011. Защита информации. Техника защиты информации. Интерфейсы взаимодействия с нейросетевыми преобразователями биометрии код доступа. М.: СтандартИнформ. 2012. 102 с.
3. Саяркин В.А., Виноградов В.Р., Парашук И.Б. Контроль эффективности и надежности системы комплексной безопасности для обеспечения защищенности доверенных иммерсивных интерфейсов взаимодействия робота и оператора // Экстремальная робототехника. 2024. № 1(35). С. 27-31.

УДК 621.396.4

#### ОСОБЕННОСТИ ФУНКЦИОНИРОВАНИЯ ИНТЕРНЕТА ВЕЩЕЙ В ЦЕНТРАХ ОБРАБОТКИ ДАННЫХ

**Грибков Владимир Александрович, Михайличенко Николай Валерьевич,  
Титов Владимир Степанович, Шарко Геннадий Васильевич**

Военная академия связи им. Маршала Советского Союза С. М. Буденного  
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия  
e-mails: 23esn2008@rambler.ru, shgorg@mail.ru, gribkov.1949@mail.ru

**Аннотация.** Статья посвящена влиянию Интернета вещей (IoT) на дата-центры. Рассмотрены ключевые аспекты интеграции IoT, включая автоматизацию управления, энергоэффективность и предиктивную аналитику. Особое внимание уделено граничным вычислениям и DCIM-системам, оптимизирующим работу ЦОД. Показано, что IoT повышает отказоустойчивость и снижает затраты, а основными драйверами внедрения выступают облачные провайдеры и операторы colocation-услуг.

**Ключевые слова:** интернет вещей; IoT; ЦОД; дата-центр; автоматизация.

#### FEATURES OF THE FUNCTIONING OF THE Internet OF THINGS IN DATA CENTERS

**Gribkov Vladimir, Mikhailichenko Nikolay, Titov Vladimir, Sharco Gennady**

Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny  
(Military Academy of Telecommunications)  
3 Tikhoretsky Av, St. Petersburg, 194064, Russia  
e-mails: 23esn2008@rambler.ru, shgorg@mail.ru, gribkov.1949@mail.ru

**Abstract.** The article is devoted to the impact of the Internet of Things (IoT) on data centers. The key aspects of IoT integration, including control automation, energy efficiency, and predictive analytics, are considered. Particular

attention is paid to edge computing and DCIM systems that optimize data center performance. It is shown that IoT increases fault tolerance and reduces costs, and cloud providers and colocation service providers are the main drivers of implementation.

**Keywords:** Internet of Things; IoT; data center; data center; automation.

С развитием цифровых технологий Интернет вещей (IoT, Internet of Things) стал неотъемлемой частью современных центров обработки данных (ЦОД). IoT-устройства используются для мониторинга, управления и оптимизации работы дата-центров, повышая их энергоэффективность, безопасность и отказоустойчивость. Однако интеграция IoT в дата-центры имеет свои особенности, связанные с масштабированием, безопасностью и управлением большими объемами данных.

Интернет вещей, активно обсуждаемый в последнее время, существенно влияет на развитие дата-центров. Широкое распространение IoT-решений не только увеличивает потребность в вычислительных мощностях и объемах хранения данных, но и меняет сами принципы архитектуры ЦОД. Чтобы сократить задержки при обработке информации в реальном времени, были разработаны новые подходы — такие как «туманные» вычисления и периферийные (граничные) дата-центры.

Кроме того, IoT-технологии позволяют значительно автоматизировать управление и оптимизировать процессы в дата-центрах. Специалисты считают ЦОД одними из самых перспективных направлений для цифровизации на основе Интернета вещей [1].

Внедрение интернета вещей в дата-центрах выходит далеко за рамки простой установки сенсоров для мониторинга оборудования. Для полноценной работы IoT-решений требуется:

- многоуровневая инфраструктура сбора, хранения и обработки данных;
- системы предиктивной аналитики, способные не только фиксировать текущее состояние ЦОД, но и прогнозировать развитие событий.

Технологии Интернета вещей открывают путь к принципиально новым моделям управления ЦОД. Такой подход предполагает:

1. Системный анализ статистических данных от множества дата-центров.
2. Использование облачных мощностей для обработки информации.
3. Переход к предикативным методам контроля инфраструктуры.

Как отмечают эксперты, управление на основе данных позволяет: повысить отказоустойчивость инфраструктуры, улучшить показатели SLA, а также оптимизировать нагрузку на технический персонал.

Функциональность, которую сегодня связывают с Интернетом вещей, уже частично реализована или постепенно внедряется в современных DCIM-системах (Data Center Infrastructure Management). Эти решения обеспечивают контроль и планирование ресурсов, оптимизацию температурных режимов и энергопотребления, а также снижение общей стоимости владения дата-центром.

По мере того, как дата-центры превращаются в крупные промышленные объекты, растёт спрос на технологии мониторинга и управления их инфраструктурой. Этим направлением активно занимаются как разработчики DCIM-решений, так и операторы коммерческих ЦОД, предлагая собственные варианты реализации.

Долгое время DCIM-системы использовались преимущественно в высокоорганизованных дата-центрах крупных корпораций. Однако с повсеместным переходом на модель аренды ИТ-ресурсов и снижением экономической эффективности содержания собственных ЦОД, основной спрос на комплексные DCIM-решения теперь исходит от операторов colocation-услуг и крупных облачных провайдеров [2].

Операторы дата-центров активно используют расширенные возможности DCIM-систем для создания дополнительных сервисов, повышения маржинальности бизнеса и привлечения клиентов. В отличие от них, облачные провайдеры чаще отказываются от готовых коммерческих решений в пользу собственных разработок, которые точнее соответствуют их специфическим требованиям и бизнес-задачам.

Активное развитие распределенных микроЦОД, стимулируемое внедрением IoT-платформ, создает спрос на усовершенствованные системы управления инфраструктурой ЦОД. Эти решения должны обладать функционалом для работы в условиях децентрализованных архитектур.

Можно отметить области применения интернета вещей базирующихся на использовании ресурсов центров обработки данных.

Умная планета. Предполагается создание цифровой платформы, которая будет аккумулировать и обрабатывать данные об экологии с различных датчиков — спутниковых, авиационных, морских и наземных, расположенных в разных точках планеты. Открытый доступ к этим данным получают граждане, государственные институты и бизнес-структуры. Платформа обеспечит мониторинг, отчетность и верификацию экологических показателей практически в реальном времени, что поможет оперативно реагировать на глобальные климатические изменения.

В качестве стартового этапа запущен пилотный проект, направленный на изучение масштабов уничтожения тропических лесов.

Ключевые возможности платформы. Мониторинг в режиме, близком к реальному времени — оперативное отслеживание изменений в экосистемах. Верификация данных — контроль достоверности поступающей информации. Раннее предупреждение — выявление глобальных климатических изменений для своевременной адаптации.

Умный город. Современные города активно внедряют цифровые решения для автоматизации различных сфер городского хозяйства, включая системы безопасности, транспортную инфраструктуру, энергоснабжение, ЖКХ, а также социальные сферы — здравоохранение, образование и государственное управление. Основные преимущества таких решений. Повышение эффективности городского управления. Оптимизация использования ресурсов. Улучшение качества жизни горожан. Создание единой цифровой экосистемы города.

Несмотря на пока ограниченное внедрение в городскую инфраструктуру, Интернет вещей уже кардинально меняет целые отрасли. Наиболее значительные изменения наблюдаются в сферах транспорта, энергоснабжения, коммунального хозяйства, экологического контроля, систем безопасности, городских информационных сервисов и решений для автоматизации быта [3].

Использование сотовых сетей для IoT-решений набирает глобальную популярность благодаря их доступности и распространенности. В перспективе смартфоны горожан смогут образовать масштабируемую сеть городских сенсоров. Уже сегодня ведутся разработки по интеграции датчиков в мобильные устройства для автоматического мониторинга экологических показателей (загрязнение воздуха, радиационный фон), полностью исключающие необходимость участия пользователей.

Умный дом. Система «Умный дом» представляет собой комплекс высокотехнологичных решений для автоматизации жилого пространства. Ее функционал охватывает управление инженерными системами здания, включая: климатическое оборудование (отопление, вентиляция, кондиционирование), осветительные приборы и электроснабжение, системы безопасности и видеонаблюдения, мультимедийные устройства.

Дата центры играют критически важную роль в функционировании современных умных домов:

- облачные вычисления: большинство современных систем умного дома используют облачные сервисы для хранения данных и сложных вычислений;
- хранение данных: ЦОД хранят огромные объемы информации от датчиков умного дома (до 1 ТБ данных в год для продвинутой системы);
- обработка в реальном времени: анализ данных с камер наблюдения, датчиков движения и других устройств часто происходит в ЦОД;
- машинное обучение: алгоритмы ИИ, улучшающие работу умного дома, обучаются и работают в дата-центрах.

Можно отметить ряд проблем, возникающих при функционировании «умных систем»:

1. Задержки связи: критически важные системы требуют минимального времени доступа к базам данных.
2. Безопасность данных: умные дома становятся мишенью для хакеров.
3. Энергопотребление: рост числа умных устройств увеличивает нагрузку на ЦОД.
4. Надежность: зависимость от интернет-соединения и работы облачных сервисов.

Таким образом, Интернет вещей трансформирует работу центров обработки данных, делая их более умными, энергоэффективными и безопасными. Однако успешное внедрение IoT требует решения проблем масштабируемости, безопасности и интеграции с облачными сервисами. В ближайшие годы развитие технологий 5G, облачные вычисления и ИИ еще больше усилят роль IoT в ЦОД.

#### СПИСОК ЛИТЕРАТУРЫ

1. Парашук И.Б., Чечулин А.А. Сущность и содержание задач поиска уязвимостей интерфейсов в интересах безопасного управления беспилотными транспортными средствами «умного города» // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2020). IX Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. / Под. ред. С.В. Бачевского; сост. А. Г. Владыко, Е.А. Аникевич. СПб.: СПбГУТ, 2020. Т.1. С. 759-763.
2. Национальный стандарт РФ ГОСТ Р 52633.4-2011. Защита информации. Техника защиты информации. Интерфейсы взаимодействия с нейросетевыми преобразователями биометрия код доступа. М.: СтандартИнформ. 2012. 102 с.
3. Докучаев В.А., Кальфа А.А., Маклачкова В.В. Архитектура центров обработки данных / Под редакцией профессора В.А. Докучаева М.: Горячая линия Телком, 2021. 240 с.: ил.

УДК 004.056

### ОБЕСПЕЧЕНИЕ УСТОЙЧИВОСТИ БЛОКЧЕЙН-СИСТЕМ К УГРОЗАМ БЕЗОПАСНОСТИ НА БАЗЕ ИНТЕГРИРОВАННОГО КОМПЛЕКСА МЕТОДОВ ЗАЩИТЫ И ВЕРИФИКАЦИИ

Калинин Максим Олегович, Бушмелев Артем Сергеевич

Санкт-Петербургский политехнический университет Петра Великого

Политехническая ул., 29, Санкт-Петербург, 195251, Россия

email: kalinin\_mo@spbstu.ru, max@ibks.spbstu.ru

**Аннотация.** Предложен метод верификации транзакций для повышения безопасности блокчейн-систем путем интеграции консорциум-ориентированных правил и честной маршрутизации. Разработан механизм честной проверки, формирующий доверительные оценки поведения узлов и обнаруживающий недобросовестных участников. Адаптирован протокол консенсуса для противодействия сговору членов консорциума. Усиление приватности и устойчивости распределенного реестра обеспечено благодаря усовершенствованной честной маршрутизации, расширенной за счет добавления протокола раскрытия участника.

**Ключевые слова:** безопасность; выбор лидера; доверительная оценка; консорциум; протокол консенсуса, распределенный реестр; честная маршрутизация; Peer Prediction; Raft.

**ENSURING THE RESILIENCE OF A BLOCKCHAIN-ENABLED SYSTEM TO SECURITY THREATS  
BASED ON AN INTEGRATED COMPLEX OF PROTECTION AND VERIFICATION METHODS****Kalinin Maxim, Bushmelev Artem**

Peter the Great St. Petersburg Polytechnic University  
29 Polytechnicheskaya st., St. Petersburg, 195251, Russia  
email: kalinin\_mo@spbstu.ru, max@ibks.spbstu.ru

**Abstract.** A transaction verification method is proposed to improve the security of a blockchain-enabled system by integrating consortium-oriented rules and garlic routing. A fair verification mechanism is developed that generates trust assessments of node behavior and detects dishonest participants. A consensus protocol is adapted to counteract collusion among consortium members. Increased privacy and stability of the distributed ledger is ensured by improved garlic routing, expanded by adding an identity disclosure protocol.

**Keywords:** security; leader election; trust evaluation; consortium; consensus protocol, distributed ledger; garlic routing; Peer Prediction; Raft.

В последние годы технологии распределенного реестра, в частности блокчейн, стали одной из ключевых основ цифровой экономики и современных систем информационной безопасности. Однако, несмотря на свои преимущества, блокчейн-системы сталкиваются с рядом существенных вызовов, которые ограничивают их широкое внедрение и эффективное применение. Прежде всего, это касается вопросов обеспечения надежной защиты данных и транзакций, а также сохранения конфиденциальности и анонимности участников блокчейн-сети. Современные блокчейн-системы должны одновременно гарантировать честность и прозрачность операций, предотвращать возможность мошенничества и сговора со стороны участников, а также обеспечивать защиту от анализа трафика, который может раскрыть личность пользователей. В условиях растущего числа и усложняющихся методов атак на блокчейн-системы эти задачи становятся все более актуальными и требуют комплексного подхода к их решению. Многие существующие методы повышения защищенности блокчейн-систем ориентированы либо на повышение безопасности и доверия внутри сети блокчейна, либо на защиту приватности, но редко совмещают вместе эти важные составляющие. При этом игнорирование одного из аспектов приводит к серьезным уязвимостям: недостаток прозрачности и контроля может создавать лазейки для злоупотреблений, а отсутствие анонимности подвергает участников риску раскрытия данных и осуществления последующих атак. Таким образом, возникает необходимость разработки интегрированного решения, которое способно не только обеспечить высокую степень защищенности транзакций, но и анонимность пользователей, сохраняя при этом возможность выявления и привлечения к ответственности нарушителей.

Одной из ключевых проблем, с которой сталкиваются блокчейн-сети, является уязвимость к так называемым «атакам большинства» («атакам 51%»). Данная проблема безопасности блокчейнов возникает из-за особенностей работы механизмов консенсуса, таких как Proof-of-Work (PoW) или Proof-of-Stake (PoS), которые требуют от участников сети достижения соглашения о состоянии цепочки. Основная идея данной атаки заключается в том, что если злоумышленник получает контроль над более половины вычислительной мощности (в случае PoW) или доли стейкинга (в случае PoS), он получает возможность манипулировать работой блокчейна, что в свою очередь позволяет нарушителю переписывать транзакции, проводить двойные траты («double spending»), блокировать подтверждение новых транзакций и, в целом, даже полностью разрушить доверие к распределенному реестру. Проблема особенно актуальна для так называемых «молодых» блокчейнов, которые (на начальном этапе функционирования) ожидаемо имеют небольшое количество участников и относительно низкую вычислительную мощность или стейкинг-капитал [1]. В таких сетях злоумышленнику проще сконцентрировать необходимые ресурсы для захвата контроля над распределенным реестром. Например, в блокчейнах с небольшой хешрейтной базой атакующий может арендовать вычислительные мощности на специализированных платформах и использовать ботнеты для достижения требуемого уровня контроля. Это делает «молодые» блокчейны привлекательной целью для злоумышленников, которые могут воспользоваться уязвимостью системы для получения финансовой выгоды или отказа в работе.

Для решения проблемы небезопасности «молодых» блокчейнов предложено внедрить консорциум-ориентированные правила, где функции верификации и фиксирования блоков передаются доверенной группе участников — консорциуму. Соответственно, каждый новый блок должен быть подписан достаточным количеством членов консорциума, что исключает возможность манипулирования со стороны нарушителей безопасности и ограничивает риски злоупотреблений, а также создает стимулы для участников через систему поощрений за выполнение работы по поддержанию безопасности сети.

В области обеспечения честной верификации транзакций и устойчивости к мошенничеству традиционно используются известные алгоритмы консенсуса Proof-of-Work (PoW) и Practical Byzantine Fault Tolerance (PBFT). PoW, впервые реализованный в Bitcoin [2], обеспечивает безопасность сети за счет высокой стоимости атаки, используя вычислительные ресурсы, что препятствует злоупотреблениям. Однако PoW неприменим в «молодых» блокчейнах из-за облегченной возможности контроля ресурсов нарушителем. Кастро [3] представили алгоритм консенсуса PBFT и его вариации, ориентированные на сети, где участники известны заранее. Этот протокол обеспечивает быструю верификацию при малом числе узлов, но плохо масштабируется при увеличении числа участников и уязвим к сговору среди проверяющих. Более современные подходы, такие как Proof-of-Reputation (PoR), предложенные в [4], используют накопленную репутацию узлов для распределения доверия. Такой подход

позволяет поддерживать честность участников, поощряя ее, но создает риски формирования «репутационных мафий» из участников консорциума, которые могут захватить контроль над системой. Протокол Raft, предложенный Хуангом [5], чаще всего используется в распределенных системах, не связанных напрямую с блокчейном. Данный протокол предполагает наличие лидера, который упорядочивает транзакции, а остальные узлы повторяют за ним. Этот подход относительно прост и надежен при небольшом числе участников. Однако вся система завязана на честность одного узла — лидера консорциума: если он становится недобросовестным, вся работа консорциума может быть скомпрометирована, при этом пользователи извне никак не участвуют в процессе верификации, и оценка честности участников не предусмотрена. Решение Tendermint [6] представляет собой гибрид PBFT и Proof-of-Stake. В нем каждый участник имеет голос с определенным весом, который определяется размером его доли (stake), что добавляет гибкости в распределении влияния, но проблема остается той же — список участников фиксирован, новые верификаторы из числа обычных участников не могут быть допущены к верификации, а значит, система уязвима к координированным действиям узкого круга валидаторов.

По результатам сравнительного анализа известных методов сделан вывод, что ни одно из рассмотренных решений не обеспечивает выполнение всей совокупности задач — защиту от сговора, оценку честности участников, безопасность «молодых» блокчейнов. Данная проблематика определяет необходимость в разработке нового метода, который сочетает решение всех трех задач.

Для устранения проблем, связанных с небезопасностью «молодых» блокчейнов и рисками ограничения доступа к системе с возможностью навязывания ложной информации о ее состоянии, авторами разработан метод верификации транзакций на основе консорциум-ориентированных правил, дополненный использованием честной маршрутизации. Ключевым элементом этого подхода выступает механизм честной проверки, позволяющий формировать доверительные оценки поведения узлов и выявлять недобросовестных участников сети. Для защиты от сговора между членами консорциума внедрен адаптированный протокол консенсуса, минимизирующий влияние координированных атак. Приватность и устойчивость к сетевому анализу обеспечиваются за счет честной маршрутизации, расширенной за счет встроенного протокола раскрытия личности, в рамках которого роль доверенной третьей стороны выполняет сам блокчейн, тем самым исключая необходимость внешних арбитров.

Метод повышения безопасности и доверия в блокчейн-системах основан на применении механизма Peer Prediction для верификации транзакций в рамках системы консорциума. В качестве основы для разработки системы используется структура в работе [7], в которой описан консорциумный блокчейн с участием общественности. Однако, из-за уязвимости исходного решения в предложенной версии системы изменен алгоритм выбора лидера консорциума. В предложенном подходе для выбора лидера применен алгоритм Raft, который является более эффективным и предсказуемым в распределенных системах. Алгоритм Raft используется для выбора лидера и достижения консенсуса, что делает его более подходящим для систем с динамическим составом участников. В отличие от случайного выбора, используемого в [7], Raft гарантирует, что лидер выбран на основе явных критериев, таких как время работы узла в сети, его роли и текущего состояния системы, что позволяет избежать случайных или целенаправленных (со стороны нарушителей) изменений в структуре управления. Такой подход улучшает стабильность и предсказуемость работы консорциума, делает его более устойчивым к атакам и сбоям, а также упрощает принятие решений. Также Raft обеспечивает большую скорость в принятии решений, снижает риск разделения сети и повышает отказоустойчивость, что критически важно для эффективного и безопасного функционирования блокчейн-системы в реальных условиях.

Алгоритм формирования группы верификаторов обеспечивает децентрализованный и согласованный процесс отбора узлов для выполнения ключевых функций в блокчейн-сети. Благодаря случайному выбору кандидатов и последующему голосованию участников консорциума достигается баланс между случайностью и коллективной верификацией. Для надежной работы блокчейн-сети необходимо не только фиксировать мнения участников, но и оценивать их достоверность. Это особенно важно в условиях возможных попыток манипуляции или недобросовестного поведения. Разработанный алгоритм честной проверки обеспечивает устойчивость сети к недобросовестным проверяющим и гарантирует, что в блок будут включены только те транзакции, за которые отдали голоса большинство проверяющих с высоким уровнем доверия.

Для одновременного обеспечения конфиденциальности данных участников и возможности их отслеживания в случае необходимости предложена система честной маршрутизации для блокчейна, которая использует блокчейн как доверенную сторону, чтобы дать возможность узлам, подобным onion-маршрутизаторам, расшифровывать пакеты только при необходимости. Блокчейн в этом случае выполняет функцию раскрытия личности только по усмотрению большинства участников сети. Таким образом, получившееся решение представляет собой гибридную модель, в которой конфиденциальность обеспечивается в обычных условиях, а отслеживаемость — только в специальных случаях, когда этого требует большинство участников. Для адаптации к специфике блокчейн-сетей и повышения уровня безопасности предложенная концепция дополнена протоколом регистрации новых узлов, который позволяет гарантировать аутентификацию участников сети и их безопасное подключение к системе, и протоколом раскрытия личности, который позволяет использовать его в реальных системах. Протокол раскрытия личности активируется в случае нарушений, например, при распространении ложной информации участниками консорциума — в таких ситуациях зафиксированные данные позволяют установить, какой участник именно является нарушителем.

Разработанная блокчейн-система представляет собой интеграцию четырех ключевых компонентов: консорциумного блокчейна с динамическим выбором верификаторов, механизма оценки их честности,

чесночной маршрутизации и контролируемого раскрытия личности. Такой симбиоз позволяет одновременно поддерживать децентрализованный контроль, защищенную коммуникацию между участниками консорциумного блокчейна и возможность установления источника нарушений при необходимости.

*Исследование выполнено за счет гранта Российского научного фонда №24-11-20005, <https://rscf.ru/project/24-11-20005/>, грант Санкт-Петербургского научного фонда (договор №24-11-20005 о предоставлении регионального гранта).*

#### СПИСОК ЛИТЕРАТУРЫ

1. Kumar K, Kumar D., Baghel Sh., Arora K. Blockchain Security: Threats, Vulnerabilities and Countermeasures-A Review // Proceedings of the International Conference on Innovative Computing and Communication (ICICC 2024). SSRN Electronic Journal. January-2025.– DOI:10.2139/ssrn.5221226.
2. Nakamoto S., Bitcoin: A Peer-to-Peer Electronic Cash System [Электронный ресурс], URL: <https://bitcoin.org/bitcoin.pdf>. (Дата обращения 04.08.2025).
3. Castro M., Liskov B. Practical byzantine fault tolerance // Proceedings of the 3rd Symposium on Operating systems design and implementation (OSDI '99). USENIX Association, USA. 1999. P. 173-186.
4. Yu J. et al. Repucoin: Your reputation is your power // IEEE Transactions on Computers. 2019. Vol. 68, № 8. P. 1225-1237.
5. Huang D., Ma X., Zhang S. Performance analysis of the raft consensus algorithm for private blockchains // IEEE Transactions on Systems, Man, and Cybernetics: Systems. 2019. Vol. 50, № 1. P. 172-181.
6. Kwon J. Tendermint: Consensus without mining // Draft v. 0.6, fall. 2014. T. 1. №. 11. C. 1-11.
7. Bai Y., Hu Q., Seo S.-H., Kang K., Lee J. J. Public Participation Consortium Blockchain for Smart City Governance // IEEE Internet of Things Journal. 2022. Vol. 9, no. 3. P. 2094-2108.

УДК 004.001; 004.001.57; 004.7.001.57

### МОДЕЛИРОВАНИЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ С ПРИМЕНЕНИЕМ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ

**Карганов Виталий Вячеславович**

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mail: vitalik210277@mail.ru

**Аннотация.** Сегодня большое внимание уделяется разработке методов и средств обработки, хранения, защиты информации, осмысление семантических, логических, методологических аспектов данной проблемы, а также такому немало важному аспекту как информационная безопасность. В тезисах (материалов) доклада приведены рекомендации по разработке математической модели, которая по своей структуре и ее задачам отвечает требованиям Доктрины информационной безопасности Российской Федерации. Последующее применение модели позволит осуществлять разработку и производство программных и технических средств обеспечения информационной безопасности с применением новейших технологий.

**Ключевые слова:** информационная безопасность; система обеспечения информационной безопасности; информационная система; инновационные технологии; математическая модель; общий модуль; частный модуль; совокупность атрибутов.

### MODELING OF INFORMATION SECURITY IN AN INFORMATION SYSTEM USING INNOVATIVE TECHNOLOGIES

**Karganov Vitaly**

Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

**Abstract.** Today, much attention is paid to the development of methods and means of processing, storing, protecting information, understanding the semantic, logical, methodological aspects of this problem, as well as such an important aspect as information security. The abstract (materials) of the report provide recommendations for the development of a mathematical model that, in its structure and its objectives, meets the requirements of the Information Security Doctrine of the Russian Federation. Subsequent application of the model will allow the development and production of software and hardware to ensure information security using the latest technologies.

**Keywords:** information security; information security management system; information system; innovative technologies; mathematical model; general module; private module; set of attributes.

В условиях перехода к высокотехнологичному обществу возрастает значение информационной деятельности и информации. Развитие новых компьютерных технологий, внедрения их в повседневную жизнь человека меняет отношение к информационным процессам и ставит их на иную качественную ступень [1].

Модернизация и последующее применение инновационных технологий, электронной промышленности приводит к углубленному научному исследованию, где в качестве результата актуализируются вопросы, связанные с обеспечением национальной безопасности страны в информационной сфере. Основополагающий документ в этой области — Доктрина информационной безопасности Российской Федерации. Ее суть [2] заключается в определении стратегических целей и основных направлений обеспечения информационной безопасности (ИБ) с учётом национальных приоритетов Российской Федерации.



Стоит отметить такой факт, что, как правило, для достижения, требуемого выше аспекта (ИБ), необходимо на должном уровне поддерживать систему обеспечения информационной безопасности (СОИБ). Как показывает анализ [2-6] она представляет собой совокупность аппаратно-программных, технических и организационных защитных мер, функционирующих под управлением СОИБ и процессов осознания ИБ, инициирующих и поддерживающих деятельность по управлению ИБ.

По своему предназначению, структурно-функциональному построению СОИБ можно отнести к кибернетическим системам, характеризующимся множеством взаимосвязанных объектов, называемых элементами системы, способных воспринимать, запоминать, перерабатывать информацию, а также обмениваться ею. По природе и структуре используемых элементов в своей деятельности она является организационной системой, поскольку по своей функциональной составляющей, СОИБ создается внутри информационной системы (ИС).

При этом заметим, что как в любой другой системе ее управляемыми объектами являются человеческие ресурсы, которые в той или иной мере связаны напрямую с ее работоспособностью. Принимая во внимание данное утверждение, а также результаты ряда [1, 3, 5, 7, 8], то для реализации и разработки требуемой математической модели (ММ) было использовано формализованное описание происходящих функций, которые возлагаются на создание и проектирование СОИБ. Сравнительный анализ для каждой функции показал их идентичность и универсальность используемых в них математических методов, что позволяет дать обобщенную формализованную запись для всех автоматизируемых функций. Предлагаемый целевой функционал по своей общности и полноте рассмотренных в нем функций можно использовать для разработки ММ исследуемого объекта исследования с использованием инновационных технологий. Декомпозиция и детализация результатов проведенных исследований позволило получить структуру ММ ИС на основании выявленных функций и процессов СОИБ.

Модель включает математические описания трех общих модулей — модуля входной и выходной информации, модуля процесса планирования и модуля процесса совершенствования, а также шести частных модулей воздействия угроз ИБ на рассматриваемую систему и аппаратно-программные средства, применяемые в СОИБ в рамках исследования ИС.

Общий модуль входной и выходной информации эквивалентен всей совокупности баз данных ИС с хранящейся в них информацией, требуемой для СОИБ.

Общий модуль процесса планирования отражает анализ и проектирование способов (методов) обработки рисков ИБ, которые описывают процедуру запуска нового процесса обеспечения ИБ, либо модернизации существующего. При создании этого процесса следует разработать методику категорирования информационных активов и формальной оценки рисков на основе данных об актуальных для рассматриваемой информационной инфраструктуры угрозах и уязвимостях.

Общий модуль процесса совершенствования СОИБ описывает результаты ранее проведенного мониторинга функционирующих процессов СОИБ, а также делает возможным реализацию корректирующих и превентивных действий в ИС.

Группа частных модулей имитирующие отрицательные воздействия угроз ИБ на рассматриваемую систему и аппаратно-программные средства, применяемые в СОИБ в рамках исследования ИС, в частности:

- частный модуль надежности средств защиты информации, применяемых в системе;
- частный модуль точной оценки вероятности компрометации и живучести системы и направлений шифрованной связи. Его работа заключается в получении аналитических оценок, которые дают возможность оптимизировать сети направления шифрованной связи в ИС с точки зрения обеспечения их максимальной живучести в зависимости от топологии сети, экзemplарности ключевой документации и количества узлов связи;
- частный модуль воздействия выявленных угроз ИБ. Оценивается по интегральному показателю — вероятности функциональной полноты контроля защищенности СОИБ, под которой понимается вероятность своевременного и достоверного обнаружения, идентификации, локализации средств защиты информации в системе обеспечения ИБ;
- частный модуль модели оценки ИБ на основе процессов. Его принцип работы, отображается совокупностью атрибутов: мероприятий процесса, входных и выходных, управления, ресурсов;
- частный модуль оценки вероятности несанкционированного доступа к конфиденциальной информации, циркулирующей в сети. Позволяет получить количественную оценку вероятности ущерба от утечки конфиденциальной информации по всем техническим каналам утечки информации семи уровневой модели взаимодействия открытых систем объекта информатизации;
- частный модуль уровня ИБ на основе модели зрелости процессов. Основу которой составляют идентифицированные атрибуты оцениваемых процессов, представляющие измеримые характеристики возможностей того или иного процесса, и методы их оценивания.

Таким образом, полученные методические рекомендации в виде ММ для обеспечения ИБ в ИС представляют совокупность описаний способов задания, оценки и контроля обеспечения уровня ИБ, разрабатываемых в виде моделей угроз, защиты с учетом критериев и показателей обеспечения ИБ. Данная модель отображает наиболее существенные стороны функционирования ИС в реальных условиях боевой обстановки. В модели дополнительно учтены воздействия как внешних, так и внутренних факторов обстановки на все основные элементы системы, являющейся объектом исследования, и, в первую очередь, на систему сбора данных с использованием инновационных технологий.

## СПИСОК ЛИТЕРАТУРЫ

1. Волкова В.Н. Теория информационных процессов и систем / В.Н. Волкова // 2-е изд., пер. и доп. Учебник и практикум для вузов. 2024. 432 с.
2. Доктрина информационной безопасности Российской Федерации, утверждённая Указом Президента РФ от 5 декабря 2016 г. № 646.
3. Карганов В.В. Глава 1. Основные понятия, общеметодологические принципы технологии защиты информации в условиях кибернетического противоборства // Технологии защиты информации в условиях кибернетического противоборства. Костарев С.В., Карганов В.В., Липатников В.А. СПб.: ВАС. 2020. С. 29-67.
4. Малюк А.А. Теория защиты информации: научная литература М.: Горячая линия Телеком, 2020. 184 с.
5. Карганов В.В. Формирование модели предметной области для информационной системы / В.В. Карганов, В.О. Драчев, Г.Н. Левченко // Инновационные технологии и технические средства специального назначения Труды десятой общероссийской НПК. 2018. С. 264-268.
6. ГОСТ Р ИСО/МЭК 27001-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. М.: Стандартинформ, 2021.
7. Карганов В.В. Методология безопасности информации в текущих информационных системах / В.В. Карганов // Национальная безопасность России: актуальные аспекты. Сб. избр. статей Всероссийской научно-практической конференции. СПб.: 2020. С. 21-27.
8. Лукашенко, В.И. Роль искусственного интеллекта в информационной безопасности / В.И. Лукашенко, Р.В. Яровой // Региональная информатика и информационная безопасность. Сборник трудов Санкт-Петербургской международной конференции и Санкт-Петербургской межрегиональной конференции. Санкт-Петербург, 2024. С. 121-124.

УДК 004.056

**ИНФОРМАЦИОННО-ТЕОРЕТИЧЕСКИЙ АНАЛИЗ КАНАЛОВ СВЯЗИ:  
МЕТРИКИ ЗАЩИЩЁННОСТИ И ПРЕДЕЛЫ ПРИМЕНИМОСТИ****Клишин Александр Владимирович, Яровой Роберт Владимирович**

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: tms65xx@yandex.ru, Nadzar@yandex.ru

**Аннотация.** В тезисе представлены ключевые метрики — энтропия, взаимная информация, кросс-энтропия, избыточность, маскируемость — позволяющие выявлять статистические закономерности и зоны уязвимости потока. Подчёркнуты как достоинства подхода, так и его ограничения в условиях асимметричной информации и высокоуровневых атак.

**Ключевые слова:** информационная безопасность; теория информации; энтропия; взаимная информация; защищённость каналов связи; вероятностные модели; телекоммуникационные сети; криптоустойчивость.

**INFORMATION-THEORETICAL ANALYSIS OF COMMUNICATION CHANNELS:  
SECURITY METRICS AND APPLICABILITY LIMITS****Klishin Alexander, Yarovoy Robert**

Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: tms65xx@yandex.ru, Nadzar@yandex.ru

**Abstract.** The thesis presents key metrics — entropy, mutual information, cross-entropy, redundancy, maskability — that allow identifying statistical patterns and areas of vulnerability of the flow. Both the advantages of the approach and its limitations in the conditions of asymmetric information and high-level attacks are emphasized.

**Keywords:** information security; information theory; entropy; mutual information; communication channel security; probabilistic models; telecommunication networks; cryptographic resistance.

Безопасность коммуникационных каналов всё чаще рассматривается не как инженерная, а как вероятностная задача, требующая формализации. Теория информации предоставляет инструментарий, способный количественно описывать подверженность потока перехвату, исходя из статистических характеристик — вне зависимости от используемого протокола или алгоритма [1].

Энтропия, как мера неопределённости, фиксирует внутреннюю хаотичность сигнала. Избыточность служит зеркальной метрикой, показывая, насколько поток отличается от равновероятного шума. Взаимная информация демонстрирует степень зависимости между оригиналом и наблюдаемым выходом: чем выше её значение, тем легче восстановить исходную структуру сообщения [2].

Сопутствующие метрики — кросс-энтропия, пороговая энтропия, индекс маскируемости — позволяют более тонко оценивать предсказуемость и возможность извлечения закономерностей. Анализ энтропийной плотности даёт динамическую картину: локализацию уязвимых зон, особенно в каналах с переменной структурой.

Преимущества подхода заключаются в его независимости от языка, реализации алгоритма и возможности автоматизированного мониторинга. Метод способен выявлять угрозы даже при полном отсутствии доступа к ключам или спецификациям шифра [3].

Однако существуют и ограничения. Во-первых, метод игнорирует семантику: он не способен обнаружить утечку смысла, если та не сопровождается статистической аномалией. Во-вторых, в условиях частичного знания о канале возможны ложные выводы — особенно при наличии асимметричного шума. В-третьих, атаки, имитирующие легитимные потоки, слабо детектируются статистическими средствами, если построены на близком к равномерному распределению.

Тем не менее, совмещение информационных метрик с эвристическим и поведенческим анализом позволяет выстраивать адаптивные системы оценки защищённости, способные функционировать в реальном времени.

Таким образом, разворачивается новый уровень анализа, в котором защищённость определяется не столько алгоритмом, сколько формой данных. В этом контексте метрики становятся не только индикаторами компрометации, но и средствами диагностики архитектурной уязвимости каналов.

#### СПИСОК ЛИТЕРАТУРЫ

1. Солодухин Б.В., Рябов Г.А., Боголепов Г.С., Яровой Р.В. Подход к решению задачи оптимального выбора программных средств защиты информации в автоматизированных системах управления // Национальная безопасность России: актуальные аспекты. Сборник избранных статей Всероссийской научно-практической конференции. СПб, 2021. С. 31-36.
2. Добрышин М.М., Диденко П.М. Оценка защищённости беспроводных сетей связи // Радиотехника, электроника и связь («РЭС-2013»). Сборник докладов II Международной научно-технической конференции. ОАО «ОНИИП». 2013. С. 155-160.
3. Марков Я.А. К вопросу о способах дешифрования классических шифров // Безопасные информационные технологии. Сборник трудов Двенадцатой международной научно-технической конференции. Москва, 2023. С. 165-169.

УДК 004.056.5

#### DDOS-АТАКИ НА ТЕЛЕКОММУНИКАЦИИ: УЯЗВИМОСТИ И СТРАТЕГИЯ ЗАЩИТЫ

**Клишин Александр Владимирович, Яровой Роберт Владимирович**  
Военная академия связи им. Маршала Советского Союза С. М. Буденного  
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия  
e-mails: tms65xx@yandex.ru, Nadzar@yandex.ru

**Аннотация.** В тезисе представлены ключевые векторы угроз, особенности протокольных уязвимостей и эффективные меры противодействия — от фильтрации трафика и DPI до машинного обучения и scrubbing-центров. Подчёркнута необходимость перехода к проактивной модели устойчивости.

**Ключевые слова:** DDoS-атаки; телекоммуникационные сети, операторы связи; киберустойчивость; сигнальные протоколы; машинное обучение; сетевой трафик; нейтрализация угроз.

#### DDOS ATTACKS ON TELECOMMUNICATIONS: VULNERABILITIES AND DEFENSE STRATEGY

**Klishin Alexander, Yarovoy Robert**  
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny  
3 Tikhoretsky Av, St. Petersburg, 194064, Russia  
e-mails: tms65xx@yandex.ru, Nadzar@yandex.ru

**Abstract.** The paper presents key threat vectors, protocol vulnerability features, and effective countermeasures — from traffic filtering and DPI to machine learning and scrubbing centers. It emphasizes the need to move to a proactive resilience model.

**Keywords:** DDoS attacks; telecommunication networks; telecom operators; cyber resilience; signaling protocols; machine learning; network traffic; threat mitigation.

DDoS-атаки представляют собой не попытку компрометации данных, а сознательное разрушение доступности услуг, и в телекоммуникационной среде проявляют себя особенно разрушительно. Асимметрия обработки сетевого трафика, отсутствие аутентификации на уровне протокольных шлюзов и архитектурная сложность делают инфраструктуру операторов связи уязвимой к перегрузкам [1].

Сетевые и транспортные уровни атакуются SYN/UDP/ICMP-флудом, IP-фрагментацией, RST- и ACK-флудом, что истощает ресурсы маршрутизаторов и вызывает каскадные сбои. Прикладной уровень подвержен HTTP flood, DNS amplification, SIP INVITE-флудам [2].

Уязвимости SS7, Diameter и SIP-протоколов — следствие проектирования в эпоху доверенных сетей. Злоумышленник способен перегружать сигнальные каналы и инициировать ложные команды маршрутизации. Дополнительную угрозу представляют CDN, DNS, BRAS/BNG, находящиеся на границе сети, принимающие первый удар и часто лишённые адекватной защиты [3].

IoT-ботнеты (Mirai, Hajime, Mozi) обеспечивают геораспределённую генерацию терабитного трафика. В сочетании с Fast Flux, DGA и мультивекторностью они создают атаки, к которым не применимы шаблоны реагирования. Микросегментация и контроль трафика east-west часто отсутствуют, что усиливает внутреннее распространение атак [4].

Комплексная защита требует гибридной модели. Поведенческий анализ выявляет скрытые шаблоны активности. Машинное обучение распознаёт аномалии в структуре трафика. Протоколы NetFlow, IPFIX и sFlow позволяют агрегировать метаданные без сохранения содержимого, сохраняя масштабируемость.

Сигнатурный и эвристический анализ актуален на ранних стадиях, а DPI — на поздних, при необходимости анализа высокоуровневых шаблонов. Трафик фильтруется с помощью BGP FlowSpec и RTBH, а scrubbing-центры и DDoS Protection-as-a-Service обеспечивают предварительную очистку данных.

Дополняют защиту honeypot-системы, выявляющие инструменты и тактики атакующих. Ключевой элемент — интеграция событий в SIEM-платформы и корреляция с внешними источниками данных об угрозах. Только такой подход обеспечивает устойчивость в условиях постоянно эволюционирующих сценариев DDoS.

Экономически оправданной оказывается не реакция, а профилактика. Поддержка защищенности телеком-сетей требует стратегической архитектуры, в которой устойчивость достигается не мощностью оборудования, а глубиной адаптивной защиты.

#### СПИСОК ЛИТЕРАТУРЫ

1. Яровой Р.В., Кривоногова Е.В., Рябов Г.А. Атаки на веб-приложения: определение, типы и профилактика // Тенденции развития науки и образования. 2023. № 101-4. С. 96-98.
2. Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетевых войнах начала XXI века // Санкт-Петербург, 2017.
3. Аманжолов О.М. Исследование методов и средств обнаружения DDoS-атак // Молодой ученый. 2023. № 50 (497). С. 5-8.
4. Попов А.О. Анализ методов обнаружения и защиты от DDoS-атак в автоматизированных системах // В сборнике: Актуальные проблемы авиации и космонавтики. Сборник материалов X Международной научно-практической конференции, посвященной 100-летию академика М.Ф. Решетнева и Дню космонавтики. В 3-х томах. Красноярск, 2024. С. 274-276.

УДК 681.142

#### НЕКОТОРЫЕ АСПЕКТЫ НЕОБХОДИМОСТИ МОДЕЛИРОВАНИЯ СИСТЕМ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

**Ковалев Игорь Станиславович, Пантюхин Олег Игоревич,  
Логинов Вячеслав Алексеевич, Ногин Сергей Борисович**

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: iskova@yandex.ru, p\_oleg99@mail.ru, loginov64@rambler.ru, sprintnsb@mail.ru

**Аннотация.** Единственным путем достижения цели совершенствования систем специального назначения является их моделирование. С этой целью применяются аналитические и имитационные модели, каждая из которых имеет свои преимущества и свои недостатки. Крайне важным также является оценка эффективности полученных в ходе моделирования результатов.

**Ключевые слова:** система специального назначения; моделирование; аналитическая и имитационная модели; оценка эффективности моделирования.

#### SOME ASPECTS OF THE NEED FOR SPECIAL PURPOSE SYSTEM MODELING

**Kovalev Igor, Pantyukhin Oleg, Loginov Vyatcheslav, Nogin Sergey**

Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: iskova@yandex.ru, p\_oleg99@mail.ru, loginov64@rambler.ru, sprintnsb@mail.ru

**Abstract.** The goals of improving special-purpose systems can be achieved only through modeling. For this purpose, analytical and simulation models are used, each of which has its advantages and disadvantages. It is also extremely important to evaluate the effectiveness of the results obtained during the simulation.

**Keywords:** special purpose system; modeling; analytical and simulation models; evaluation of modeling effectiveness.

Системы специального назначения (ССН), безусловно, относятся к классу сложных организационно-технических систем. Поэтому для достижения цели своего функционирования она должна иметь в своем составе (и, естественно, имеет) систему управления, которая представляет собой совокупность функционально взаимосвязанных органов управления (лица, принимающие решения), размещающихся на специальном образе оборудованных пунктах управления, оснащенных средствами управления (средствами связи и автоматизации) [1].

Необходимость совершенствования таких систем обусловлена периодически проявляющимися в ходе их функционирования несоответствиями, совокупность которых однозначно указывает на наличие проблемы, как несоответствие между существующим и требуемым положением дел в ССН. Следует помнить, что «правильно сформулированная проблема — наполовину решенная проблема».

Из всего вышесказанного следует, что совершенствование систем специального назначения является исключительно важным и актуальным, особенно в настоящее время.

Понятно, что чем масштабнее и дороже предполагаемые мероприятия по совершенствованию ССН, тем абсолютно недопустимы в них так называемые «волевые решения». При этом становится еще более очевидным важность применения современных научных методов, которые позволят оценить возможные последствия абсолютно каждого решения, отбросить неправильные, а рекомендовать исключительно лучшее, как с точки зрения достижения цели функционирования системы специального назначения, так и минимизации затрат на его реализацию. Следует помнить, что при этом крайне опасно полагаться только лишь на интуицию и собственный опыт.

В функционирующих ССН проведение натурного эксперимента практически всегда невозможно, поэтому единственным способом обеспечения их совершенствования является моделирование.

Главная идея моделирования системы специального назначения состоит в создании ее модели и проведении эксперимента, но уже с моделью. После чего, на основе анализа данных, полученных в результате моделирования, вырабатываются предложения и рекомендации по совершенствованию уже, собственно, ССН [2, 3].

Для разработки адекватных моделей специалистами в этой области выработаны ряд основополагающих принципов и рекомендации, главными из которых являются:

- соответствие разрабатываемой модели целям исследования; соответствие между сложностью модели и точностью результатов моделирования;
- соразмерности погрешностей моделирования;
- модульности построения моделей;
- открытости модели;
- коллективности разработки модели [1, 2].

Учитывая главную идею моделирования и следуя указанным рекомендациям, можно выделить задачи моделирования, которые, как правило, выполняют в следующей последовательности.

Сначала необходимо предельно ясно и четко сформулировать и конкретизировать цель (цели) моделирования, что позволит разработать постановку задачи на сам процесс моделирования системы специального назначения.

Далее следует приступить к разработке самой модели. Этот процесс начинается, прежде всего, с создания концептуальной модели функционирования ССН, причем именно в аспекте цели моделирования.

После чего, на основе этой концептуальной модели разрабатывается математическая модель и, в заключение, программная реализация самой модели системы специального назначения.

Затем необходимо провести исследование системы специального назначения уже на ее модели. Сущность такого исследования состоит в тщательном и детальном планировании и проведении эксперимента.

И в заключении проводится самый скрупулезный анализ и тщательная обработка полученных результатов моделирования, на основе которых вырабатываются предложения и рекомендации по совершенствованию ССН, т.е. полученные в ходе моделирования результаты переносятся на реальную систему специального назначения.

Известно, что математические модели бывают аналитическими и имитационными [1, 2].

Аналитические модели сложных систем, обычно, имеют значительную степень упрощения реальности и абстрагирования. Аналитическая форма моделирования применяется, как правило, для предварительной оценки значений характеристик системы специального назначения на ранних стадиях ее совершенствования, когда информации для построения более точной модели по объективным причинам еще недостаточно. По результатам аналитического моделирования можно сделать вывод о правильности принятой концепции совершенствования ССН, что иногда и бывает достаточным. Погрешность таких моделей порядка 20%, что вполне нормальный результат для этих целей.

Но с появлением вычислительных машин появилась возможность проводить имитационное моделирование. Идея имитационного моделирования состоит в многократном повторении процесса функционирования системы специального назначения в зависимости от проявления случайных внутренних и внешних, как правило неблагоприятных, воздействий. Главным преимуществом имитационного моделирования является его более высокая точность и огромная область применимости, что обуславливает более широкие возможности по комплексному моделированию сложных систем, а значит и систем специального назначения. При этом, что крайне важно, его погрешность значительно меньше погрешности аналитического моделирования и обычно составляет не более 10 %.

Понятно, что эффективность применения модели любого класса в целом определяется следующими показателями:

- ее адекватностью (совпадением свойств модели и соответствующих свойств моделируемого объекта);
- точностью моделирования;
- достоверностью и полнотой исходных данных;
- стабильностью исследуемой системы, дающей основания утверждать, что время исследования пренебрежимо мало по сравнению со временем существенного изменения ее параметров.

Очевидно, что выполнение таких условий возможно лишь приближенно, что приводит к погрешности результатов, в связи с чем возникают ограничения на применение той или иной модели в различных условиях, в том числе в конкретных условиях обстановки.

Математические модели наряду с расчетными и информационными задачами в современных условиях являются важнейшим и, как правило, единственным инструментом повышения эффективности принимаемых решений по направлениям совершенствования систем специального назначения в целом, а значит и их систем управления.

Применение методов моделирования для принятия обоснованных решений по совершенствованию ССН невозможно без оценки их эффективности, которая также осуществляется на основе моделирования.

При этом оценка эффективности может осуществляться как априорно, в этом случае говорят об оценке эффективности решений на совершенствование системы, так и апостериорно, когда оценка эффективности функционирования систем специального назначения проводится с учетом внедрения выработанных предложений по ее совершенствованию [1, 3].

#### СПИСОК ЛИТЕРАТУРЫ

1. Иванов А.Ю. Теория принятия решений: учебное пособие / А.Ю. Иванов, В.И. Комашинский, О.И. Пантюхин. СПб: СПбГУТ, 2023.
2. Теория военного управления. Учебное пособие / Под ред. С.В. Чернякова СПб: ВАС, 2024.
3. Кондрашов Ю.В. и др. Моделирование и проектирование систем: Части I и II. СПб.: ВАС, 2023.

УДК 004.056.5

**ОЦЕНКА ЗАЩИЩЕННОСТИ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ: ОБЩИЕ ВОПРОСЫ И ДЕТАЛИЗАЦИЯ ЦЕЛЕЙ И ОБЪЕКТОВ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРИМЕРЕ СИСТЕМЫ ОЧИСТНЫХ СООРУЖЕНИЙ ВОДОКАНАЛА****Котенко Игорь Витальевич<sup>1</sup>, Саенко Игорь Борисович<sup>1</sup>, Паращук Игорь Борисович<sup>1,2</sup>**<sup>1</sup> СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 194064, Россия,

<sup>2</sup> Военная академия связи им. Маршала Советского Союза С. М. Буденного, Тихорецкий пр-т, д. 3, Санкт-Петербург, 194064, Россия

e-mails: ivkote@comsec.spb.ru, ibsaen@comsec.spb.ru, shchuk@rambler.ru

**Аннотация.** В рамках детализации описания этапов и сущности оценки защищенности сложных систем, сформулированы современные методологические и практические аспекты, характеризующие цели, задачи и объекты одного из важнейших систематических этапов такой оценки — аудита информационной безопасности. Цели и объекты аудита информационной безопасности рассмотрены на примере системы очистных сооружений водоканала, как типичной критической инфраструктуры. Предполагается, что своевременное проведение аудита позволит выявить все слабые места в информационной безопасности критических систем такого класса, позволит обезопасить процесс функционирования промышленным систем очистки воды от атак злоумышленников.

**Ключевые слова:** оценка защищенности, критическая инфраструктура, аудит, система очистных сооружений, цель, данные.

**ASSESSMENT OF CRITICAL INFRASTRUCTURE SECURITY: GENERAL ISSUES AND DETAILING OF THE GOALS AND OBJECTS OF INFORMATION SECURITY AUDIT USING THE EXAMPLE OF A WATER TREATMENT SYSTEM****Kotenko Igor<sup>1</sup>, Saenko Igor<sup>2</sup>, Parashchuk Igor<sup>1,2</sup>**<sup>1</sup> St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), 39, 14-th Linia, VI, St. Petersburg, 199178, Russia<sup>2</sup> Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny, 3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: ivkote@comsec.spb.ru, ibsaen@comsec.spb.ru, shchuk@rambler.ru

**Abstract.** In the context of detailing the description of the stages and essence of the assessment of the security of complex systems, modern methodological and practical aspects are formulated that characterize the goals, objectives and objects of one of the most important systematic stages of such an assessment — information security audit. The goals and objects of information security audit are considered using the example of a water treatment plant system as a typical critical infrastructure. It is assumed that timely audit will identify all the weak points in the information security of critical systems of this class, will protect the process of functioning of industrial water treatment systems from intruder attacks.

**Keywords:** security assessment, critical infrastructure, audit, wastewater treatment system, purpose, data.

Работу современной критической инфраструктуры, любого современного высокотехнологичного предприятия, например, такого, как система очистных сооружений водоканала (СОСВ), невозможно себе представить без встроенной или взаимодействующей с данной системой IT-платформы. Данная IT-платформа призвана решить ряд информационных и вычислительных задач, ведь бизнес-процессы и технологические процессы, реализуемые в рамках критической инфраструктуры подобного рода постоянно автоматизируются, причем, данные обычно хранятся в виртуальном пространстве, а сотрудникам предоставляется возможность работать дистанционно. В этой связи одной из важнейших задач на сегодняшний день является надежная защита данных, хранящихся, обрабатываемых и циркулирующих по телекоммуникационным каналам и трактам в рамках современной критической инфраструктуры [1–4].

Актуальность данной задачи обусловлена, кроме прочего, ежегодным активным пополнением списка методов негативных воздействий и способов атак на IT-платформы, безудержным ростом перечня уязвимостей разнородных критических информационных и телекоммуникационных ресурсов. Обязательным элементом организации надежной защиты данных, хранящихся, обрабатываемых и циркулирующих по телекоммуникационным каналам и трактам в рамках современной критической инфраструктуры, является оценка ее защищенности. При этом одной из ключевых форм, одним из наиболее эффективных подходов к оценке защищенности считается своевременный аудит информационных систем, аудит безопасности инфраструктуры компании в целом, включая облачные хранилища [5].

Именно поэтому в современных условиях, когда речь идет о СОСВ, все более ценными становятся данные, без которых управление и нормальное функционирование таких критически важных систем становится невозможным, а, значит, аудит информационной безопасности играет непреходящую роль в обеспечении надежной защиты подобной информации. Цель аудита информационной безопасности СОСВ, как критической инфраструктуры, состоит в обеспечении конфиденциальности, целостности и доступности информации, необходимой для управления и эффективного функционирования подобной организации.

Для достижения поставленной цели аудита, и, в конечном итоге, для решения проблемы анализа и повышения защищенности СОСВ, необходимо объединение опыта научных исследований в области кибербезопасности, экологического мониторинга и анализа данных. В рамках аудита информационной безопасности СОСВ, как критической инфраструктуры, должен быть исследован и оценен уровень защиты от несанкционированного доступа, утечки данных, атак со стороны злоумышленников и других угроз. Эта оценка может быть как точечной, так и интервальной [6, 7].

Более того, аудит также поможет в обеспечении соблюдения законодательных требований и стандартов безопасности. Таким образом, аудит информационной безопасности СОСВ представляет собой процесс систематической проверки, оценки и детального анализа информационных систем и процессов, направленный на выявление уязвимостей и рисков, связанных с безопасностью данных, а также дальнейшее предоставление рекомендаций по их устранению и улучшению.

Основными киберугрозами для современных СОСВ, как критических инфраструктур, являются: вмешательство (проникновение) хакеров в элементы и процедуры ИТ-платформы критической системы и кража конфиденциальной информации; скрытые враждебные программы, которые способны долгое время существовать на ИТ-платформе критической системы незаметно, собирая аналитику работы подсистем, а затем неожиданно «обрушить» критическую инфраструктуру; утечка персональных данных сотрудников, смежников, подрядчиков или клиентов подобной критической инфраструктуры; инсайдерские провокации, например, продажа коммерческой тайны конкурентам; DDoS-атаки, способные обрушить телекоммуникационные каналы и тракты, предназначенные для обмена данными в рамках СОСВ; «заражение» данных вирусами, фишинг и инструменты социальной инженерии; потеря данных из-за аппаратных сбоев, неисправностей, катастроф.

Объектами аудита информационной безопасности современных СОСВ, как критических инфраструктур, могут выступать: сайты и веб-приложения; информационные подсистемы и СУБД; сетевые службы и сервисы (электронная почта, служба удаленных рабочих столов, VoIP, FTP и другие); сетевое оборудование; беспроводные сети; средства контроля безопасности информации, анализа движения и защиты информации (DLP); серверные и пользовательские операционные системы; резервные копии, логика и регламент копирования; прикладное программное обеспечение; документация и регламенты, касающиеся информационной безопасности систем очистки воды.

Предполагается, что аудит информационной безопасности СОСВ, как критических инфраструктур, поможет: собирать данные для формирования перспективного плана будущих работ по улучшению подсистем защиты информации; понять уровень состояния и тенденции развития информационной безопасности инфраструктуры, а также получить аргументированную оценку защищенности системы от различного рода угроз; избежать утечки конфиденциальной информации и защитить ИТ-платформу СОСВ от действий злоумышленников; снизить влияние человеческого фактора в критических аспектах информационной безопасности; определить необходимые инвестиции в безопасность и обосновать их для руководства; избежать рисков потерь репутации, связанных с низким уровнем защищенности конфиденциальной информации.

Таким образом, в рамках детализации описания этапов и сущности оценки защищенности сложных систем, сформулированы современные методологические и практические аспекты, характеризующие цели, задачи и объекты одного из важнейших систематических этапов такой оценки — аудита информационной безопасности. Цели и объекты аудита информационной безопасности рассмотрены на примере СОСВ, как критической инфраструктуры. Предполагается, что своевременное проведение аудита позволит выявить все слабые места в информационной безопасности критических систем такого класса, позволит обезопасить процесс функционирования промышленным систем очистки воды от атак злоумышленников.

*Исследование выполнено за счет гранта Российского научного фонда № 23-11-20024, <https://rscf.ru/project/23-11-20024/>, и Санкт-Петербургского научного фонда.*

#### СПИСОК ЛИТЕРАТУРЫ

1. Ерохин С.Д., Петухов А.Н., Пилюгин П.Л. Управление безопасностью критических информационных инфраструктур. СПб.: Горячая линия - Телеком. 2024. 240 с.
2. Макаренко С. И. Аудит безопасности критической информационной инфраструктуры. Учебное пособие. СПб.: Научные технологии, 2023. 122 с.
3. Котенко И.В., Саенко И.Б., Парашук И.Б. Уровни архитектуры компонентов оперативной оценки защищенности информационных и телекоммуникационных ресурсов критической инфраструктуры // Информационная безопасность регионов России (ИБРР-2023) XIII-я Санкт-Петербургская Межрегиональная конференция. Санкт-Петербург, 25-27 октября 2023 г., Материалы конференции, СПб.: СПОИСУ, 2023. С.88-90.
4. Setola R., Luijff E., Theoharidou M. Critical Infrastructures, Protection and Resilience // Managing the Complexity of Critical Infrastructures / Studies in Systems, Decision and Control. Springer, 2016. pp. 1-18.
5. Парашук И.Б., Саенко И.Б., Пантюхин О.И. Анализ состояния исследований по моделированию разграничения доступа к информации в облачных инфраструктурах критически важных информационных систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция (АПИНО-2018); сб. науч. ст. в 4 т. / Под. ред. С.В. Бачевского и др. СПб.: СПбГУТ, 2018. Т.1. С. 604-609.
6. Котенко И.В., Парашук И.Б. Интервальный анализ защищенности телекоммуникационных ресурсов критически важных инфраструктур // Математические методы в технологиях и технике. Сборник трудов Международной научной конференции ММТТ-35. №1, 2022. СПб.: Издательство Политехнического университета. 2022. Том 1. С. 64-67.
7. Котенко И.В., Парашук И.Б. Информационные и телекоммуникационные ресурсы критически важных инфраструктур: особенности интервального анализа защищенности // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2022. №2. С. 33-40.

УДК 621.396.4

**ДОСТУП ПОЛЬЗОВАТЕЛЕЙ К ЭЛЕКТРОННЫМ ОБРАЗОВАТЕЛЬНЫМ РЕСУРСАМ  
И ЭЛЕКТРОННОЙ ДИДАКТИЧЕСКОЙ ИНФОРМАЦИИ ПО КАНАЛАМ СВЯЗИ ОБЩЕГО  
ПОЛЬЗОВАНИЯ: СУЩНОСТЬ, ЦЕЛИ И КРИТЕРИИ АУДИТА БЕЗОПАСНОСТИ****Крюкова Елена Сергеевна, Паращук Игорь Борисович**

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: e.krukovaa69@yandex.ru, shchuk@rambler.ru

**Аннотация.** В докладе рассмотрена специфика и условия функционирования каналов связи общего пользования, использующихся в интересах безопасного доступа пользователей к электронным образовательным ресурсам и электронному дидактическому (учебно-педагогическому) контенту. Определены ключевые концептуальные основы аудита безопасности, исследованы современные взгляды на сущность, цели и задачи многокритериального аудита защищенности процедур и объектов такого класса. Сформулированы базовые критерии, обязательные к реализации в рамках аудита безопасности каналов доступа и самих электронных ресурсов, что позволит на научной основе синтезировать алгоритмы оптимального и адаптивного наблюдения, оценивания и прогнозирования состояния их защищенности в различных условиях обстановки.

**Ключевые слова:** электронные образовательные ресурсы; каналы связи; защищенность; аудит безопасности; критерий; параметр информационной безопасности.

**USER ACCESS TO ELECTRONIC EDUCATIONAL RESOURCES AND ELECTRONIC DIDACTIC  
INFORMATION VIA PUBLIC COMMUNICATION CHANNELS: NATURE,  
OBJECTIVES AND CRITERIA OF SECURITY AUDIT****Kryukova Elena, Parashchuk Igor**

Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: e.krukovaa69@yandex.ru, shchuk@rambler.ru

**Abstract.** The report examines the specifics and conditions of operation of public communication channels used in the interests of secure user access to electronic educational resources and electronic didactic (educational and pedagogical) content. The key conceptual foundations of security audit are defined, modern views on the essence, goals and objectives of multi-criteria security audit of procedures and objects of this class are studied. Basic criteria are formulated that are mandatory for implementation within the framework of the security audit of access channels and the electronic resources themselves, which will allow, on a scientific basis, to synthesize algorithms for optimal and adaptive monitoring, assessment and forecasting of their security status in various conditions.

**Keywords:** electronic educational resources; communication channels; security4 security audit; criterion; information security parameter.

Анализ особенностей и итогов реального использования современных средств и методов многокритериального аудита в различных областях промышленности, телекоммуникаций и в иных сферах народного хозяйства, опыт изучения текущего состояния информационного обеспечения образовательной деятельности на nive подготовки инженерных кадров, синопсис нынешних требований по информационной безопасности и направлений технической эволюции электронных образовательных ресурсов (ЭОР), изучение тенденций модификации подходов к созданию и обработке электронной дидактической информации (ЭДИ), доступной пользователям по каналам связи общего пользования (КСОП), а также широкое использование эффективного симбиоза преимуществ информатики и телекоммуникаций, позволили сформулировать актуальную систему предположений, гипотез и суждений по поводу сущности многокритериального аудита информационной безопасности (МАИБ) в интересах защищенного доступа пользователей к электронным образовательным ресурсам и электронному дидактическому (учебно-педагогическому) контенту по каналам связи общего пользования [1, 2].

Многокритериальный аудит информационной безопасности каналов связи, предназначенных для доступа к ЭОР и аудит защищенности смыслового и семантического содержания ЭДИ представляет собой единый комплекс руководимых из единого штаба аудита, взаимосвязанных систематических и целенаправленных мероприятий (организационных, технологических и технических), основанный на непрерывном либо периодическом (регулярном) наблюдении за состоянием уровня защищенности данных процедур и объектов, качественном или количественном оценивании параметров информационной безопасности и прогнозировании изменений состояния информационной безопасности под влиянием конструктивных или деструктивных факторов. Общая идея многокритериального аудита информационной безопасности каналов связи, предназначенных для доступа к ЭОР к контенту ЭДИ — это единая система точек зрения и базовых принципов, детально характеризующих методологию и генеральную линию всепроникающего и всеобъемлющего, текущего и прогностического контроля информационной безопасности процедур и объектов такого класса.

Информационная безопасность каналов связи общего пользования, предназначенных для доступа к ЭОР и контенту ЭДИ — свойство или совокупность специальных характеристик этих процессов и компонентов,



обуславливающих защищенность передающих трактов КСОП, а также информационная безопасность сущности и содержания потоков информации, передаваемых по подобным каналам в интересах образовательной деятельности. Информационная безопасность каналов связи общего пользования для доступа к ЭОР и ЭДИ, обуславливает необходимость проверки информации, хранящейся в локальной сети образовательной организации, необходимость аудита нежелательной информации, аудита содержания электронной почты образовательной организации и иные операции [3, 4].

Под состоянием информационной безопасности каналов связи общего пользования, предназначенных для доступа к ЭОР и контенту ЭДИ, традиционно понимают множество параметров и показателей, численно характеризующих защищенность этих процедур и объектов исследований в конкретный момент времени. Проще говоря, состояние информационной безопасности каналов связи общего пользования, ЭОР и ЭДИ — вектор параметров информационной безопасности в параметрическом пространстве состояний, описывающих защищенность каналов и ресурсов [5].

Фундаментальной целью многокритериального аудита информационной безопасности каналов связи, предназначенных для доступа к ЭОР и контенту ЭДИ, является безопасное информационное обеспечение системы образования, адекватное целям функционирования и управления ею и учитывающее влияние внешних и внутренних, конструктивных и деструктивных факторов. Существенную, принципиальную основу многокритериального аудита информационной безопасности каналов связи, предназначенных для доступа к ЭОР и контенту ЭДИ, должны составлять, и составляют ключевые критерии, обязательные к соблюдению в рамках реализации политики безопасности системы образования, включая механизмы многофакторной аутентификации пользователей и разграничения прав их доступа [6]:

- критерии, обуславливающие единство подходов к МАИБ в интересах защищенного доступа пользователей к электронным образовательным ресурсам и электронному дидактическому (учебно-педагогическому) контенту по каналам связи общего пользования;

- критерии, характеризующие целевую ориентацию (целенаправленность) МАИБ в интересах защищенного доступа пользователей к электронным образовательным ресурсам и электронному дидактическому (учебно-педагогическому) контенту по каналам связи общего пользования;

- критерии, определяющие информационно-аналитическое единство МАИБ в интересах защищенного доступа пользователей к электронным образовательным ресурсам и электронному дидактическому (учебно-педагогическому) контенту по каналам связи общего пользования, данные критерии является мерилем, ориентированным на использование стандартных единых расчетно-аналитических подходов к реализации аудита и единых процедур агрегации контрольной информации;

- критерии, предопределяющие регулярность МАИБ в интересах защищенного доступа пользователей к электронным образовательным ресурсам и электронной дидактической информации, и заключающиеся в проведении процедур наблюдения, оценивания и прогнозирования показателей информационной безопасности в соответствии с периодами, обусловленными целями, задачами и возможностями оценочной деятельности для конкретных задач обеспечения соблюдения политики безопасности;

- критерии, регулирующие вопросы комплексности (целостности, всесторонности, интегративности) МАИБ в интересах защищенного доступа пользователей к ЭОР и контенту ЭДИ.

Таким образом, проведен анализ специфики и условий функционирования каналов связи общего пользования, использующихся в интересах безопасного доступа пользователей к электронным образовательным ресурсам и электронному дидактическому (учебно-педагогическому) контенту. Определены ключевые концептуальные основы аудита безопасности, исследованы современные взгляды на сущность, цели и задачи многокритериального аудита защищенности процедур и объектов такого класса. Предпринята попытка сформулировать базовые критерии, обязательные к реализации в рамках аудита безопасности каналов доступа и самих электронных ресурсов, что позволит на научной основе синтезировать алгоритмы оптимального и адаптивного наблюдения, оценивания и прогнозирования состояния их защищенности. Это, в свою очередь, создает предпосылки для синтеза алгоритмов оптимального и адаптивного наблюдения, оценивания и прогнозирования состояния защищенности каналов связи для доступа к ЭОР и ЭДИ в целях снижения затрат ресурсов для решения конкретных задач обеспечения соблюдения политики безопасности системы образования в различных условиях обстановки.

#### СПИСОК ЛИТЕРАТУРЫ

1. Паниокова С.В. Цифровые инструменты и сервисы в работе педагога. Учебно-метод. пособие. М.: Изд-во «Про-Пресс», 2020. 33 с.
2. Шамиев В.А., Крюкова Е.С., Паращук И.Б. Электронный контент цифровых образовательных ресурсов как основа информационного обеспечения подготовки специалистов наукоемких профессий // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 13 / СПОИСУ. СПб.: 2024. С. 68-70.
3. Ганжур А.П., Отакулов А.С., Дьяченко Н.В. Политика безопасности контента // Молодой исследователь Дона. №6 (33), 2021. С. 41-44.
4. Котенко И.В., Паращук И.Б. Информационные и телекоммуникационные ресурсы критически важных инфраструктур: особенности интервального анализа защищенности // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2022. №2. С. 33-40.
5. Севрюкова Е.А. Надзор и контроль в сфере безопасности: учебник для вузов / под общей редакцией В.И. Каракеяна. 2-е изд., испр. М.: Издательство Юрайт, 2025. 340 с.
6. Паращук И.Б., Сундуков В.А. Этапы разработки моделей и методов многофакторной аутентификации пользователей как элементов политики разграничения прав доступа к ресурсам инфокоммуникационных сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2023). XII Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. / Под. ред. С.И. Макаренко. СПб.: СПбГУТ, 2023. Т. 1., С. 833-837.

УДК 621.396.6

**ПРИМЕНЕНИЕ МОБИЛЬНЫХ БАЗОВЫХ СТАНЦИЙ GSM В СОВРЕМЕННЫХ СИСТЕМАХ СВЯЗИ И БЕЗОПАСНОСТИ****Кузоятов Владислав Валерьевич, Юдин Анатолий Алексеевич**

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: vvforever2@mail.ru, ytol5@mail.ru

**Аннотация.** В докладе рассматривается анализу применения подвижных станций GSM, возможность их применения в вооружённых силах Российской Федерации. Рассмотрены варианты применения станций GSM, ключевые направления развития. Методологическая основа включает анализ статистических данных и опыт применения станций GSM в условиях чрезвычайных ситуаций, массовых мероприятий, зоне проведения СВО. Предложены варианты применения в интересах межвидовой системы информационного обмена. Полученные результаты могут быть полезны для представителей органов военного управления, занимающихся внедрением и развитием межвидовой системы информационного обмена.

**Ключевые слова:** межвидовая система обмена информацией; мобильные станции GSM; 5G; система оповещения; массовое внедрение станций 5G mmWave; система видеонаблюдения; динамическое перераспределение ресурсов; система идентификации; быстрое развёртывание; работа в основных диапазонах.

**THE USE OF GSM MOBILE BASE STATIONS IN MODERN COMMUNICATION AND SECURITY SYSTEMS****Kuzoyatov Vladislav, Iudin Anatolii**

Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: vvforever2@mail.ru, ytol5@mail.ru

**Abstract.** The report examines the use of GSM mobile stations and the possibility of their use in the armed forces of the Russian Federation. The options for using GSM stations and key areas of development are considered. The methodological framework includes the analysis of statistical data and experience in the use of GSM stations in emergency situations, mass events, and the area of their implementation. Possible applications in the interests of an interspecific information exchange system are proposed. The results obtained may be useful for representatives of military authorities involved in the implementation and development of an interspecific information exchange system.

**Keywords:** interspecific information exchange system; GSM mobile stations; 5G; notification system; mass introduction of 5G mmWave stations; video surveillance system; dynamic resource redistribution; identification system; rapid deployment; operation in the main ranges.

С целью организации сотовой связи в неподготовленных местах, в рамках передачи голоса и ещё более актуальной — передачи данных по сетям 3G и 4G возможно применение специальных мобильных решений, позволяющих в короткий промежуток времени развернуть базовую станцию на базе различных шасси. В качестве основы может быть использован автомобиль с цельнометаллическим кузовом или КУНГом, внутри которых смонтирована аппаратура связи GSM — стандарта, а также мощная раскладная или сборная мачта, на которой устанавливаются панельные секторные антенны сотовой связи, а также радиорелейная антенна для связи (привязки) со стационарными базовыми станциями существующей сети. В состав передвижного комплекса сотовой связи необходимо включение дизельного генератора для автономности энергоснабжения системы связи. В кабине с аппаратурой должен быть расположен комплект аккумуляторных батарей (АКБ) для резервирования питания в случае остановки дизельного генератора. Скорость развёртывания мобильной базовой станции (МБС) зависит от сложности сборки антенн, а также от местности, на которой предполагается работа станции, и подготовленности личного состава, обслуживающего комплекс [1, 2].

Другим вариантом исполнения, может является вариант размещения МБС на базе автомобильного прицепа или контейнера. Такая компоновка удешевляет общую стоимость МБС, даёт возможность большей мобильности и автономности комплекса. Состав оборудования займёт 1-2 стойки размером 27 U, а антенные модули могут быть представлены тремя панельными секторными GSM антеннами и одна дополнительная антенна радиорелейной станции [3].

Радиус действия МБС составляет до 25 км, а одна такая станция позволяет обслужить до нескольких тысяч абонентов. При выборе системы подключения к базовой сети сотовой связи передвижные станции могут также использовать, оптоволоконное или радиорелейное оборудование.

Применение МБС позволит обеспечить связь стандарта GSM каждому военнослужащему, находящемуся в зоне покрытия, а значит предоставить командирам всех степеней резервные каналы связи, а также возможность функционирования межвидовой системы информационного обмена. В условиях проведения специальной военной операции, контртеррористической операции, в условиях воздействия БпЛА, данные станции могут быть задействованы в целях оповещения личного состава и местного населения в рамках организации противовоздушной обороны [4].

Мобильные базовые станции представляют собой мобильные телекоммуникационные комплексы, способные оперативно развёртывать сети сотовой связи в зонах с отсутствующей или поврежденной инфраструктурой. В настоящее время МБС активно применяются в:

- крупных мероприятиях (массовые события, фестивали);
- удалённых районах (геологоразведка, строительные проекты).

Современные МБС эволюционировали от простых ретрансляторов до интеллектуальных мультисервисных платформ с поддержкой 4G/LTE и готовностью к 5G.

Технологические возможности:

- поддержка всех современных стандартов (2G/3G/4G, перспектива 5G);
- возможность работы в диапазонах 900/1800/2100 МГц;
- пропускная способность до 100 Мбит/с на абонента;
- встроенные системы криптозащиты передачи данных.

Мультистандартная поддержка:

- 2G (GSM/GPRS/EDGE): обеспечение базового голосового покрытия и передачи данных (до 384 Кбит/с);
- 3G (UMTS/HSPA+): высокоскоростная передача данных (до 42 Мбит/с);
- 4G (LTE/LTE-A): поддержка скоростей до 300 Мбит/с на прием и 150 Мбит/с на передачу;
- 5G Ready: подготовка к переходу на новые стандарты (NSA/SA архитектуры).

Частотная гибкость, работа в основных диапазонах:

- 900 МГц (широкое покрытие);
- 1800 МГц (баланс покрытия/ёмкости);
- 2100 МГц (высокая пропускная способность);
- 2600 МГц (LTE-Advanced);
- возможность быстрого переключения между диапазонами.

Технические особенности. Автономность работы в экстремальных условиях, совместимость со спутниковыми каналами, защита от пыли и влаги (стандарт IP65).

Тактические преимущества. Развёртывание за 30-60 минут, защищенный режим работы с частотным хоппингом, интеграция с системами РЭБ.

В настоящее время Российский комплекс «Алтаец-М» проходит апробацию в условиях СВО и способен обеспечить связь в интересах подразделений, находящихся вне зоны покрытия оператора сотовой связи, засекреченные каналы передачи данных, устойчивость к радиоэлектронному подавлению.

Важной особенностью применения МБС в интересах МСИО — это расширенные возможности функций управления абонентской базой [5]. Динамическая регистрация и аутентификация, принудительная перерегистрация всех абонентов при развёртывании, селективная аутентификация (разрешение доступа только авторизованным пользователям), IMEI-фильтрация (блокировка нежелательных устройств), приоритизация абонентов, создание групп с разным уровнем доступа (высший приоритет: экстренные службы, командный состав, операторы БпЛА), средний приоритет: рядовые пользователи, низший приоритет: массовые подключения, функции мониторинга, количество активных абонентов, уровень сигнала каждого устройства, потребление трафика, разграничения трафика (механизмы QoS (Quality of Service), политики шейпинга трафика (ограничение скорости по: группам абонентов, типам сервисов и времени суток), глубокая фильтрация пакетов (DPI), блокировка нежелательных протоколов, приоритизация критически важных приложений, анализ и классификация трафика в реальном времени, доступ только для авторизованных SIM-карт, полная изоляция от публичных сетей, шифрование всех коммуникаций, динамическое перераспределение частот, принудительное отключение «паразитных» абонентов, аварийное освобождение каналов для спецсвязи, автоматический выбор оптимальных частот, адаптация к уровню помех, динамическое перераспределение ресурсов, комбинация с спутниковыми терминалами, использование дронов как ретрансляторов, интеграция с системами IoT.

В рамках развития МБС получают свой искусственный интеллект для управления нагрузкой и предотвращения фактов НСД, квантовое шифрование трафика, а также компактные станции на водородных элементах. В настоящее время МБС оснащаются программно-определяемым радио (SDR), станциями 5G mmWave, автономными саморазвертывающимися системами, спутниковой backhaul-связью для работы в абсолютно глухих зонах, дронами-ретрансляторами с целью расширения зоны покрытия, блокчейном для аутентификации абонентов. Подвижные GSM-станции трансформируются из узкоспециализированного оборудования в универсальные телекоммуникационные платформы.

Таким образом в интересах Вооружённых сил Российской Федерации целесообразно создание мобильных сетевых кластеров, способных формировать временную телеком-инфраструктуру в полевых условиях, тем самым обеспечивая резервирование основных каналов связи, функционирования систем оповещения о воздушной обстановке и межвидовой системы информационного обмена.

#### СПИСОК ЛИТЕРАТУРЫ

1. Попов В. И., Скуднов В. А. Основы проектирования сотовых сетей мобильной связи. М. : Горячая линия Телеком, 2024. 400 с.
2. Буснюк Н. Н., Мельянец Г. И. Системы мобильной связи : учебное пособие для СПО. Санкт-Петербург : Лань, 2022. 128 с.
3. Берлин А. Н. Сотовые системы связи : учебное пособие. М. : БИНОМ. Лаборатория знаний (Интернет-Университет ИТ), 2012. 359 с.
4. Ефремов Г. Россияне создали первую отечественную базовую 5G [Электронный ресурс]. URL: <https://cnews.ru/link/a643856> (дата обращения: 02.10.2025).
5. Билятинов К. З., Арсеньева А. З., Меняйло В. В., Ивановский С. В. Основы построения и функционирования мобильных систем передачи данных : учебное пособие. Санкт-Петербург : Университет ИТМО, 2023. 157 с.

УДК 004.056.5

**ПРОБЛЕМА ЗАЩИТЫ ОТ МНОГОХОДОВЫХ СОЦИО-ИНЖЕНЕРНЫХ АТАК.  
АНАЛИЗ ОСНОВНЫХ ЭЛЕМЕНТОВ****Кюнер Андрей Павлович, Чечулин Андрей Алексеевич**  
СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия

e-mails: kunerandrey@mail.ru, andreych@bk.ru

**Аннотация.** При разработке мер противодействия угрозам информационной безопасности, исходящим от социальной инженерии авторы научных работ фокусируют внимание на изучении защитных механизмов потенциальной жертвы, включающих организационные, технические средства защиты, а также его личные качества и психологический портрет. Целью осуществления социо-инженерной атаки является нарушение информационной безопасности путем воздействия на слабое звено — неподготовленного пользователя. При этом наиболее сильным элементом в системе защиты информации является подразделение по информационной безопасности и его специалисты. Для обеспечения эшелонированной защиты сотрудников от киберугроз необходимо разработать меры противодействия атакам на различных стадиях, ведущую роль в этом процессе играют специалисты в области информационной безопасности.

**Ключевые слова:** социо-инженерная атака, целевая кибератака, основные этапы, компьютерные преступления, мониторинг.

**PROBLEM OF DEFENSE AGAINST MULTI-STEP SOCIAL ENGINEERING ATTACKS.  
ANALYSIS OF THE MAIN ELEMENTS****Kyuner Andrey, Chechulin Andrey**

St. Petersburg Federal Research Center of the Russian Academy of Sciences

39 14th Line VO, St. Petersburg, 199178, Russia

e-mails: kunerandrey@mail.ru, andreych@bk.ru

**Abstract.** In order to develop measures to counter information security threats from social engineering, the authors of scientific articles focus on studying the defensive mechanisms of a potential victim, including organizational means and tools, as well as his personal qualities and psychological profile. The aim of a social engineering attack is to violate information security by targeting the weakest link — the unprepared person. At the same time, the strongest element in the information security system is the security department and its specialists. To ensure multilayered protection of employees from cyber threats, it is necessary to develop measures to counter attacks at various stages, with information security specialists playing a leading role in this process.

**Keywords:** social engineering attack, targeted cyberattack, main stages, computer crime, monitoring.

Стремительное развитие информационных технологий предоставляет гражданам широкий спектр возможностей и услуг. Вместе с тем всестороннее использование инновационных технологий порождает определенные риски утечки данных, использования технологий злоумышленниками. Основная проблема заключается в том, что при создании новой технологии обработки и передачи данных анализ уязвимостей и внедрение средств защиты проводятся после распространения технологии [1]. Обеспечение информационной безопасности частных лиц, организаций и общества в целом является задачей государственного уровня. В контексте информационной безопасности социальная инженерия занимает одно из ключевых значений в тактиках злоумышленников. К особенностям применения методов социальной инженерии можно отнести не только использование человеческого фактора как наиболее уязвимого элемента в информационной системе [2, 3], но и применение данных методов в качестве инструментов обхода любых, даже наиболее продвинутых средств защиты информации [4].

Значительная доля информационных ресурсов предлагает организационные и программные меры защиты от подобных угроз. К таким мерам можно отнести: усиленную аутентификацию, обучение, использование антивирусных утилит, обновление программного обеспечения [5–6]. Указанные меры направлены на усиление последней линии защиты — пользователя, противодействиям предпосылкам реализации атаки уделяется недостаточно внимания.

В целях разработки методики противодействия социо-инженерным атакам необходимо прежде всего разделить данную область на составные элементы и этапы атаки. К составным элементам относятся:

- атакующий (цели, мотивы, квалификация, ресурсы, знания, сценарии, технические средства);
- канал (электронная почта, телефонная связь, физический контакт и др.);
- атакуемый (уязвимости, защитные механизмы, уровень доступа).

К основным стадиям (этапам) атаки можно отнести:

- подготовка (сбор сведений, разработка сценария, выбор жертв, подготовка технических средств);
- построение доверия (установление связи, психологическое воздействие);
- выполнение действий (обход защиты, выполнение цели атаки);
- завершение (получение результата, сокрытие следов, анализ эффективности метода).

Внедрение средств защиты информации подразумевает повышение устойчивости пользователя к атакам [7], изучению параметров нарушителя и повышению защищенности канала передачи данных уделяется, как правило, меньше внимания [8]. В тоже время внедрение защитных мер сосредоточено на этапе построения доверия (как

правило, организационными мерами) и пресечении выполнения действия (путем использования антивирусного программного обеспечения или других средств). Защита пользователя на этапах, предшествующих построению доверия, не рассматривается, как и изучение параметров атакующего. Вывод: совершенствование механизмов защиты от социо-инженерных атак должно быть основано на изучении модели нарушителя, повышении защищенности среды передачи данных, разработке мероприятий по выявлению атак на начальных стадиях.

Наиболее эффективным инструментом, позволяющим оперативно принимать решения по защите от кибератак, является центр мониторинга и реагирования. К функциям мониторинга можно отнести: поиск сведений о компании и ее сотрудников, выявление утечек данных, анализ новых угроз и тактик атаки, настройка механизмов оповещения об инцидентах и их расследование, разработка способов предотвращения атак. При тщательном изучении основных стадий атаки можно определить закономерность на первый взгляд случайных событий. Примером такой закономерности могут послужить события в обществе, например, начало приемной кампании в учебных заведениях. Для специалиста по кибербезопасности будет очевиден сценарий мошеннических действий, когда злоумышленники станут предлагать помощь в поступлении на бюджетные места за вознаграждение. Оповещение о новых методах атак значительно снижает число потенциальных жертв.

На основе автобиографических сведений, данных мониторинга, анализа атак, сведений об информационных системах организации, активов компании, доступа сотрудников к конфиденциальной информации можно определить категории лиц, подверженных социо-инженерным атакам, вероятные сценарии и каналы связи между злоумышленником и жертвой.

Наличие перечня потенциальных объектов атак и сведений об основных угрозах позволяет осуществить выбор средств защиты от социо-инженерных атак в дополнении к уже существующим. Если система защиты информации позволяет уменьшить до минимума угрозу атаки и нормативные правовые документы не требуют разработки дополнительных защитных мер, то средств защиты от социальной инженерии полностью основываются на базовых средствах, внедренных в информационную систему предприятия. В теории информационной безопасности средствами достижения заданных целей могут послужить такие понятия, как модель безопасности с полным перекрытием, изолированная среда и принцип нулевого доверия. На практике достижение указанного эффекта не всегда возможно, поэтому необходимо рассмотреть возможность внедрения защитных мер на каком-либо из этапов атаки. Трудоемкой задачей является пресечение предпосылок к реализации кибератаки, поэтому необходимо повысить защищенность общего канала связи злоумышленника и жертвы, наличие которого обязательным условием осуществления контакта. Каждый канал характеризуется возможностями по передаче информации, которые определяют перечень возможных атак, а также встроенными средствами защиты. При рассмотрении примера взаимодействия через средства мгновенного обмена сообщениями наличие и активация функции белого списка абонентов предотвращает установление контакта со злоумышленником, за исключением случаев использования скомпрометированных учетных записей.

При выборе средств защиты существует определенный ряд критериев (стоимость, удобство, техническая реализуемость и др.) по которому выбирается средство. Если средство защиты информации представляет собой комплекс программных или аппаратных средств и его внедрение невозможно по тем или иным причинам, то организационные меры применяются в качестве альтернативы техническим [9]. Завершающим этапом является тестирование, сопровождение разработанных инструментов защиты мониторинг выявления новых угроз.

Таким образом, представленные меры позволяют сосредоточить внимание на проведении профилактических мероприятий, не требующих построения сложной системы защиты пользователя. Усовершенствование методов защиты основывается не на дорогостоящих организационных (таких, как программы обучения персонала) и программных мерах (комплексные средства антивирусной защиты, защиты от несанкционированного доступа), а на мероприятиях, целью которых является противодействие различным этапам атаки силами и средствами подразделений по информационной безопасности.

#### СПИСОК ЛИТЕРАТУРЫ

1. Методы и средства обеспечения безопасности информации [Электронный ресурс]. // Режим доступа к ресурсу URL: <https://intuit.ru/studies/courses/3609/851/lecture/31660?page=3> (дата обращения: 29.07.2025).
2. Alharthi, Dalal & Regan, Amelia. Social Engineering Defense Mechanisms: A Taxonomy and a Survey of Employees' Awareness Level, 2020 С. 521-541. 10.1007/978-3-030-52249-0\_35.
3. Воробьева А.А. Методика анализа инцидентов социальной инженерии / А.А. Воробьева, Е.А. Воробьева // Журнал высоких гуманитарных технологий. 2025. № 1(8). С. 60-73.
4. Киберугроза №1, или как бороться с социальной инженерией [Электронный ресурс]. // Режим доступа к ресурсу URL: <https://www.securitylab.ru/analytics/500877.php> (дата обращения: 29.07.2025).
5. Кюннер А.П. Особенности противодействия методам социальной инженерии специалистами по информационной безопасности в рамках центров мониторинга и реагирования / А.П. Кюннер // Информатизация и связь. 2025. № 2. С. 97-101. DOI 10.34219/2078-8320-2025-16-2-97-101.
6. Исследование механизмов социальной инженерии и анализ методов противодействия / В.Ю. Евлевский, М.М. Путято, А.С. Макарян, И.В. Володин // Электронный сетевой политематический журнал «Научные труды КубГТУ». 2021. № 2. С. 57-68.
7. Наумова К.Д., Радугин В.Ю. Исследование основных методов противодействия атакам, основанным на методах социальной инженерии, на предмет их эффективности и применимости к современной ситуации в РФ // Инновационные механизмы управления цифровой и региональной экономикой. Материалы V Международной студенческой научной конференции. Москва, 2023. С. 145-158.
8. Солодяников А. В. Методы защиты от атак методами социальной инженерии / А. В. Солодяников, В. В. Сухостат, Л. С. Антонова // Региональная информатика и информационная безопасность : сборник научных трудов, Санкт-Петербург, 01–03 ноября 2017 года / Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления. Том Выпуск 3. СПб: СПОИСУ, 2017. С. 206-210.
9. Новикова Е.Ф., Хализев В.Н. Разработка модели угроз для объектов критической информационной инфраструктуры с учетом методов социальной инженерии. DOI: 10.21672/2074-1707.2019.48.4. С. 127-135. Прикаспийский журнал: управление и высокие технологии, № 4 (48). г. Краснодар. 2019. С. 127-135.

УДК 004.056

**УСКОРЕНИЕ ТАКТИЛЬНОГО ИНТЕРНЕТА С ПОМОЩЬЮ ПРОТОКОЛА QUICK UDP INTERNET CONNECTIONS: ВОПРОСЫ БЕЗОПАСНОСТИ И КОНФИДЕНЦИАЛЬНОСТИ****Лаута Олег Сергеевич, Митрофанов Михаил Валерьевич**

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

Университет ИТМО

Кронверкский пр., 49, Санкт-Петербург, 197101, Россия

e-mails: laos-82@yandex.ru, vonafortim@andex.ru

**Аннотация.** Рассматривается ситуация, как транспортный протокол Quick UDP Internet Connections может ускорить развитие тактильного интернета в сетях шестого поколения с точки зрения безопасности и защиты персональных данных. Протокол обеспечивает сквозное шифрование и быстрое установление соединения без дополнительного обмена сообщениями. Проведена систематизация основных угроз и уязвимостей, важная для приложений с крайне малой задержкой передачи данных: атаки на этап установления соединения, повторная отправка перехваченных сообщений, навязывание неподдерживаемой версии протокола, подделка запросов и злоупотребление переносом соединения, истощение вычислительных ресурсов сервера, атаки «распределенный отказ в обслуживании», отслеживание пользователей по служебным маркерам и идентификация посещаемых сайтов по сигналам трафика. Описаны практические меры защиты: полная шифровка первого сообщения клиента в протоколе защиты транспортного уровня, механизмы противодействия повторной отправке, принудительная проверка подлинности клиента перед выделением ресурсов, ограничение режима быстрого запуска соединения, фильтрация и ограничение скорости обработки пакетов, а также использование методов обезличенного протокола передачи гипертекста и многоцелевого подуровня приложений поверх зашифрованного транспорта. Сформулированы направления дальнейших исследований и проверки на экспериментальных стендах в сетях пятого и шестого поколения.

**Ключевые слова:** тактильный интернет; транспортный протокол Quick UDP Internet Connections; сети шестого поколения; незамедлительное установление соединения; полная шифровка первого сообщения клиента; защита персональных данных; отказ в обслуживании; система обнаружения вторжений; многоцелевой подуровень приложений поверх зашифрованного транспорта; малая задержка передачи данных.

**ACCELERATING THE TACTILE INTERNET WITH THE QUICK UDP INTERNET CONNECTIONS TRANSPORT PROTOCOL: SECURITY AND PRIVACY PERSPECTIVE****Lauta Oleg, Mitrofanov Mikhail**

Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

University ITMO

49 Kronverksky Av, St. Petersburg, 197101, Russia

e-mails: laos-82@yandex.ru, vonafortim@andex.ru

**Abstract.** The article examines how the Quick UDP Internet Connections transport protocol can accelerate the development of tactile internet in sixth-generation networks in terms of security and personal data protection. The protocol provides end-to-end encryption and fast connection establishment without additional messaging. The main threats and vulnerabilities have been systematized, which is important for applications with extremely low data transfer latency: attacks on the connection establishment phase, re-sending of intercepted messages, forcing an unsupported protocol version, spoofing requests and abuse of connection transfer, exhausting server computing resources, distributed denial-of-service attacks, tracking users by service markers, and identifying visited websites by traffic signals. Practical protection measures are described: full encryption of the first client message in the transport layer protection protocol, mechanisms to counteract re-sending, forced client authentication before allocating resources, restriction of the quick connection startup mode, filtering and limiting the speed of packet processing, as well as the use of anonymized hypertext transfer protocol and multi-purpose application sublayer methods on top of encrypted transport. Directions for further research and testing on experimental stands in fifth and sixth generation networks are formulated.

**Keywords:** tactile internet; Quick UDP Internet Connections transport protocol; sixth-generation networks; immediate connection establishment; full encryption of the client's first message; personal data protection; denial-of-service; intrusion detection system; multi-purpose application sublayer over encrypted transport; low data transfer latency.

**Постановка задачи.** Тактильный интернет требует почти нулевой задержки передачи данных, высокой надежности и строгой защиты информации. Традиционные транспортные протоколы передают данные последовательно. Если один фрагмент теряется, следующие задерживаются. Транспортный протокол Quick UDP Internet Connections работает поверх протокола пользовательских датаграмм и одновременно передает несколько независимых потоков данных, поэтому потеря одного фрагмента не блокирует остальные. Он использует протокол защиты транспортного уровня версии 1.3, полностью шифрует данные и может начинать обмен без дополнительного обмена сообщениями при установлении соединения. Это делает его подходящим кандидатом для приложений с тактильной обратной связью, робототехникой, дополненной и виртуальной реальностью.

*Модель угроз.* Опасности концентрируются на этапе начала соединения и при обработке больших объемов данных. Нападающий может навязать нежелательную версию протокола, подделать служебные сообщения, вынудить сервер выделять ресурсы без подтверждения подлинности клиента или многократно повторять ранее перехваченные сообщения. Возможны атаки, при которых злоумышленник посылает большое количество зашифрованных пакетов по протоколу пользовательских датаграмм с целью перегрузить сеть и сервер. Отдельная линия угроз связана с приватностью: слежение за пользователями по служебным маркерам и определение посещаемых сайтов по структуре трафика даже при шифровании содержимого [1].

*Меры защиты.* Нужно полностью зашифровать первое сообщение клиента при установлении соединения, ограничить режим быстрого запуска, обязательно проверять подлинность клиента, прежде чем выделять ресурсы, и использовать механизмы противодействия повторной отправке. На периметре сети следует применять фильтрацию и ограничение скорости обработки пакетов, а также настраивать телеметрию для выявления аномалий [2]. Для повышения приватности целесообразно использовать обезличенный протокол передачи гипертекста и многоцелевой подуровень приложений поверх зашифрованного транспорта, которые разделяют знания о том, кто обращается и к какому ресурсу.

*Практическая значимость.* В сетях пятого и шестого поколения критичны целостность и подлинность сообщений управления, поскольку от них зависят устойчивость управления роботами и обучение с тактильной обратной связью. Внедрение расширенного профиля транспортного протокола с полной защитой первого сообщения клиента, ограничением режима быстрого запуска и телеметрией снижает риск сбоев сервиса и неудобств пользователей. Рекомендуется регулярно проверять устойчивость инфраструктуры к перегрузкам зашифрованным трафиком [3].

*Направления дальнейших исследований.* Следует разработать профиль безопасности транспортного протокола с учетом задержек, методику проверки приватности против атак по трафиковым признакам, экспериментальный стенд на основе сетей пятого и шестого поколения для генерации тактильных потоков и открытые наборы данных для оценки систем обнаружения вторжений на реальных сценариях атак.

#### СПИСОК ЛИТЕРАТУРЫ

1. Fitzek F. H., S.-C. Li, S. Speidel, T. Strufe, M. Simsek, and M. Reisslein, «Tactile Internet with Human-in-the Loop» in Tactile Internet. Academic Press, 2021, pp. 1-474.
2. Chiariotti F., Deshpande A. A., Giordani M., Antonakoglou K., Mahmoodi T., Zanella A., «UIC-EST: A QUIC-Enabled Scheduling and Transmission Scheme to Maximize Vol with Correlated Data Flows» IEEE Communications Magazine, vol. 59, no. 4, pp. 30-36, 2021.
3. R. Lychev, S. Jero, A. Boldyreva, and C. Nita-Rotaru, «How Secure and Quick is QUIC? Provable Security and Performance Analyses» in 2015 IEEE Symposium on Security and Privacy, 2015, pp. 214-231.

УДК 004.056.5

### К ВОПРОСУ ПОСТРОЕНИЯ ЦИФРОВЫХ ДВОЙНИКОВ И БЫСТРОГО ПРОТОТИПИРОВАНИЯ АЛГОРИТМОВ И ПРОГРАММНЫХ СРЕДСТВ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Левшун Дмитрий Сергеевич<sup>1</sup>, Котенко Игорь Витальевич<sup>1</sup>, Парашук Игорь Борисович<sup>1,2</sup>

<sup>1</sup> СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия

<sup>2</sup> Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: dmitry.levshun@gmail.com, ivkote@comsec.spb.ru, shchuk@rambler.ru

**Аннотация.** В докладе рассмотрены ключевые аспекты, ориентированные на выявление сходных черт и различий в принципах и функциональном наполнении процессов быстрого прототипирования и создания цифровых двойников алгоритмов и программных средств для моделирования и практической реализации современных систем обнаружения вторжений. Определяются пригодность прототипирования и цифровых двойников для моделирования в интересах предварительного анализа структуры систем обнаружения вторжений в конкретных условиях функционирования. Исследованы общие и специфические особенности, присущие этим технологиям цифрового проектирования систем обнаружения вторжений.

**Ключевые слова:** система обнаружения вторжений; быстрое прототипирование; цифровой двойник; цифровое проектирование; алгоритм; программное средство; принцип.

### ON THE QUESTION OF CONSTRUCTING DIGITAL TWINS AND RAPID PROTOTYPING OF ALGORITHMS AND SOFTWARE FOR INSURSION DETECTION SYSTEMS

Levshun Dmitry<sup>1</sup>, Kotenko Igor<sup>1</sup>, Parashchuk Igor<sup>1,2</sup>

<sup>1</sup> St. Petersburg Federal Research Center of the Russian Academy of Sciences

39, 14-th Linia, VI, St. Petersburg, 199178, Russia

<sup>2</sup> Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: dmitry.levshun@gmail.com, ivkote@comsec.spb.ru, shchuk@rambler.ru

**Abstract.** The report examines key aspects aimed at identifying similarities and differences in the principles and functional content of rapid prototyping processes and the creation of digital twins of algorithms and software for modeling and practical implementation of modern intrusion detection systems. The suitability of prototyping and digital twins for

modeling is determined in the interests of preliminary analysis of the structure of intrusion detection systems in specific operating conditions. General and specific features inherent in these technologies of digital design of intrusion detection systems are studied.

**Keywords:** intrusion detection system; rapid prototyping; digital twin; digital design; algorithm; software; principle.

Адекватное моделирование и качественная практическая реализация современных систем обнаружения вторжений (СОВ), представляет собой сложную и нетривиальную задачу, особенно, если речь идет о многошаговых атаках нарушителей, когда подобным системам приходится обрабатывать и анализировать большие данные [1-3].

С учетом того факта, что больших данные представляют собой колоссальные массивы гетерогенной информации, для сбора, обработки и анализа которой приходится использовать специфические, зачастую, интеллектуальные, специализированные методы и алгоритмы, составляющие основу современных «сквозных» цифровых технологий, актуальность решения задач адекватного моделирования и качественной практической реализации СОВ, на наш взгляд, не вызывает сомнений [4-6].

Несомненную практическую ценность данная задача приобретает при проектировании и создании современных многофункциональных и эффективных алгоритмов и программных средств для СОВ на объектах критической инфраструктуры. При этом практическим решением задач построения цифровых моделей, натурных и полунатурных макетов и прототипов сложных алгоритмов, программ и информационных объектов, к которым относятся алгоритмы и программные средства для адекватного моделирования и качественной практической реализации СОВ, занимается теория прототипов, а для конкретных задач технического плана, используются принципы прототипирования, реверс-инжиниринга и создания цифровых двойников. Проблемам упреждающего моделирования, предварительного анализа и проактивного оценивания работоспособности сложных алгоритмов, программ и иных объектов, посвящено большое количество работ, детальный анализ которых позволяет выделить, как наиболее рациональные, методы и средства прототипирования и создания цифровых двойников. В этой связи, на наш взгляд, необходим детальный анализ базовых понятий этих методов и средств, анализ сходства и различия в содержании и функциональном наполнении общих процессов и частных процедур прототипирования и создания цифровых двойников алгоритмов и программных средств СОВ. Под быстрым прототипированием алгоритмов и программных средств СОВ будем понимать предварительный этап разработки, как самих таких алгоритмов, так и программного обеспечения для их реализации, заключающийся в создании макета — пробной, эскизной версии алгоритмического или программного объекта для СОВ [7].

Технология цифровых двойников (Digital Twin), в отличие от прототипирования, также являясь важным средством цифрового проектирования, предусматривает создание модели («двойника») — электронной копии объектов, например, алгоритма или программного средства, помогающей оптимизировать их работу и повысить эффективность их функционирования. В интересах построения и совершенствования алгоритмов и программных средств СОВ, технология цифровых двойников призвана помочь быстрее обнаруживать алгоритмические коллапсы, программные сбои и физические проблемы, точнее предсказывать результаты этих сбоев и коллизий, и, как следствие, обеспечить производство более качественных алгоритмов и программных средств для систем обнаружения вторжений [6, 8].

Поиск сходных черт и различий в содержании и функциональном наполнении процессов быстрого прототипирования и создания цифровых двойников, позволяет отметить, что быстрое прототипирование алгоритмов и программных средств СОВ используется, чаще всего, для тестирования предлагаемых разработчиками концепт, идей, замыслов, архитектурных, алгоритмических или технологических решений с точки зрения их соответствия техническому заданию и иным требованиям, а также потенциальным условиям эксплуатации. Создание эскизных прототипов алгоритмов и программных средств СОВ, также необходимо для их заблаговременной демонстрации заказчику на начальных этапах (стадиях) процесса разработки.

Отличаясь от цифровых двойников, которые, по сути, тоже являются копиями (но более точными копиями), моделями реальных алгоритмов и программных средств, технология быстрого прототипирования дает возможность работать по этапам — сначала позволяет алгоритмисту проверить работоспособность своих идей и решений для СОВ без привлечения программистов, а на втором этапе — с привлечением непосредственных разработчиков программного обеспечения процедур обнаружения вторжений. При этом в короткие сроки, создается упрощенный прототип (макет, эскиз), который может быть на какой-то следующей стадии разработки заброшен и не станет частью готового алгоритма или программного обеспечения механизмов и интерфейсов для обнаружения вторжений. Если основное преимущество цифровых двойников заключается в оптимизации работы и повышении эффективности функционирования алгоритмов и программных средств, интерфейсов для обнаружения вторжений, то главное достоинство технологии быстрого прототипирования — экономия времени, выигрыш в оперативности.

Принципы быстрого прототипирования алгоритмов и программных средств СОВ: прототип создается только после определения целевой аудитории; в прототипе должны быть учтены основные пользовательские сценарии обнаружения вторжений; прототип всегда интерактивен, так как он направлен на проверку возможных действий пользователя; при тестировании прототипа необходимо давать минимум информации потенциальному пользователю, чем больше он сделает ошибок, тем лучше для продукта; прототип необходимо сделать максимально похожим на реальный объект — систему обнаружения вторжений.



Принципы создания цифровых двойников алгоритмов и программных средств СОВ: цифровой двойник должен иметь иерархическую структуру и включать в себя многоканальную информационную систему контроля внешней среды и состояния СОВ; цифровой двойник — многомасштабное представление виртуальной модели алгоритма или программного обеспечения СОВ; цифровой двойник должен учитывать инвариантное представление внешней среды и поведения пользователей; постоянное обучение цифровых двойников с целью повышения их адекватности; цифровой двойник содержит мультимодельное отражение реального объекта и окружающей среды; цифровые двойники учитывают подчинение и сопоставление уровней реальной СОВ; цифровые двойники учитывают и используют многоконтурное управление; наличие у цифровых двойников механизмов прогнозирования изменений внешней среды.

Таким образом, исследованы и сформулированы ключевые аспекты, ориентированные на выявление сходных черт и различий в принципах и функциональном наполнении процессов быстрого прототипирования и создания цифровых двойников алгоритмов и программных средств для моделирования и практической реализации современных СОВ. Исследованы вопросы пригодности прототипирования и цифровых двойников для моделирования в интересах предварительного анализа структуры систем обнаружения вторжений в конкретных условиях функционирования. Рассмотрены принципы, общие и специфические особенности, присущие этим технологиям цифрового проектирования систем обнаружения вторжений.

*Исследование выполнено за счет бюджетной темы FFZF-2025-0016 в ФИЦ СПб РАН.*

#### СПИСОК ЛИТЕРАТУРЫ

1. Полтавцева М.А., Лаврова Д.С. Высокопроизводительные системы обнаружения вторжений. СПб.: Инфра-Инженерия. 2023. 152 с.
2. Постоногова Д.Г. Системы обнаружения вторжений: практикум. Новосибирск: СГУГиТ, 2020. 34 с.
3. Котенко И.В. Многоагентные технологии анализа уязвимостей и обнаружения вторжений в компьютерных сетях // Защита информации. Конфидент. №2. 2004. С. 2-6.
4. Макшанов А.В., Журавлев А.Е., Тындыкарь Л.Н. Большие данные. Big Data. М.: Издательство «Лань», 2024. 188 с.
5. Парашук И.Б. Проблемы Больших Данных. Особенности и пути решения // IX-ая Санкт-Петербургская Межрегиональная конференция «Информационная безопасность регионов России 2015 (ИБРР-2015)». Материалы конференции, СПб.: СПОИСУ, 2015. С. 175-176.
6. Парашук И.Б., Салюк Д.В. Анализ особенностей и роли современных «сквозных» цифровых технологий в построении и совершенствовании техники средств связи и автоматизации управления специального назначения // Техника средств связи. №2 (158). 2022. С. 13-21.
7. Кугаевский С.С. Реверс-инжиниринг и быстрое прототипирование в машиностроении: учебно-методическое пособие. Екатеринбург: Издательство Уральского университета. 2023. 98 с.
8. Бурлаков В.В., Мясоедова Т.К. Цифровой двойник: ключ к совершенствованию бизнес-процессов телекоммуникационных компаний. Монография. М.: Солон-Пресс. 2024. 104 с.

УДК 004.056.5

#### К ВОПРОСУ МНОГОКРИТЕРИАЛЬНОГО АНАЛИЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ И СРЕДСТВ НА БАЗЕ ТЕХНОЛОГИИ ИНТЕРНЕТА ВЕЩЕЙ НА ОБЪЕКТАХ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Левшун Дмитрий Сергеевич<sup>1</sup>, Парашук Игорь Борисович<sup>1,2</sup>

<sup>1</sup> СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 194064, Россия

<sup>2</sup> Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр-т, д. 3, Санкт-Петербург, 194064, Россия

e-mails: levshun@comsec.spb.ru, shchuk@rambler.ru

**Аннотация.** Обоснованы этапы решения конкретных вопросов и сформулированы потенциальные результаты в рамках нового подхода к многокритериальному анализу информационной безопасности сетей и средств на базе технологии Интернета вещей на объектах критической инфраструктуры. Данные вопросы могут и должны быть решены в интересах обнаружения слабых мест и архитектурных дефектов с точки зрения обеспечения защищенности подсистем такого класса. Новый подход к многокритериальному анализу информационной безопасности сетей и средств на базе технологии Интернета вещей ориентирован на объединение направлений и алгоритмов статического и динамического контроля защищенности объектов критической инфраструктуры в рамках единого модельно-методологического аппарата.

**Ключевые слова:** многокритериальный анализ; информационная безопасность; технология; Интернет вещей; объект критической инфраструктуры; модель; метод.

#### TO THE QUESTION OF MULTICRITERIAL ANALYSIS OF INFORMATION SECURITY OF NETWORKS AND FACILITIES BASED ON THE INTERNET OF THINGS TECHNOLOGY AT CRITICAL INFRASTRUCTURE FACILITIES

Levshun Dmitry<sup>1</sup>, Parashchuk Igor<sup>1,2</sup>

<sup>1</sup> St. Petersburg Federal Research Center of the Russian Academy of Sciences

39, 14-th Linia, VI, St. Petersburg, 199178, Russia

<sup>2</sup> Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: levshun@comsec.spb.ru, shchuk@rambler.ru

**Abstract.** The stages of solving specific issues are substantiated and potential results are formulated within the framework of a new approach to multi-criteria analysis of information security of networks and tools based on the Internet of Things technology at critical infrastructure facilities. These issues can and should be resolved in the interests of detecting weak points and architectural defects from the point of view of ensuring the security of subsystems of this class. The new approach to multi-criteria analysis of information security of networks and tools based on the Internet of Things technology is aimed at combining the directions and algorithms of static and dynamic control of the security of critical infrastructure facilities within a single model and methodological apparatus.

**Keywords:** multicriteria analysis; information security; technology; Internet of things; critical infrastructure object; model; method.

Акцентирование вопросов информационной безопасности, как ключевых аспектов, важных приоритетов национальной безопасности в целом, обусловлено все более активным проявлением киберугроз, связанных со вмешательством во внутренние дела Российской Федерации, увеличением числа атак на российские информационные ресурсы, на ведомственные и частные инфокоммуникационные сети и системы, а также ростом числа компьютерных преступлений, совершенных с применением современных и перспективных цифровых технологий.

Одной из причин роста числа компьютерных атак является переход от автоматизации к интеллектуализации бизнес-процессов на объектах критической инфраструктуры (ОКИ), включая особенности, связанные с активным внедрением технологии Интернета вещей. Системы, использующие данные технологии, позволяют осуществлять сбор и анализ данных со всех объектов критически важной инфраструктуры, контролировать их работу и управлять ими, что позволяет повысить эффективность бизнес-процессов данных систем и вывести их на качественно новый уровень [1, 2].

Оборотная сторона этого процесса заключается в значительном увеличении ущерба, который может быть причинен посредством информационных атак. При этом последствия атак, ввиду специфики объектов критически важной инфраструктуры, могут повлечь не только финансовый ущерб и ущерб репутации компании, но также несут прямую угрозу жизни людей [3, 4].

Известные методы для многокритериального анализа (МКА) информационной безопасности сетей и средств (СиС) на базе технологии Интернета вещей (ТИВ) на ОКИ, не отвечают предъявляемым требованиям по оперативности, полноте, точности и адекватности принимаемых решений.

Во многом это объясняется отсутствием стандартов в области контроля защищенности устройств и ТИВ, непрерывным ростом количества этих устройств, а также взрывным ростом объемов передаваемых ими данных.

Более того, МКА и обеспечение информационной безопасности таких масштабных систем требуют значительных усилий по автоматизации данных процессов, в то время как действия злоумышленников становятся все более разнообразными.

Именно поэтому вопросы МКА информационной безопасности СиС на базе ТИВ на ОКИ, являются, на наш взгляд, особенно важными и актуальными. Для решения таких вопросов необходимо выработать такие научные и практические подходы, относящиеся к МКА информационной безопасности СиС на базе ТИВ на ОКИ, которые позволили бы проактивно, заранее обнаруживать слабые места с точки зрения защищенности и архитектурные дефекты в политике безопасности и структуре подобных объектов.

В ходе решения поставленных фундаментальных вопросов может и должен быть решен ряд задач, могут и должны быть получены следующие результаты:

- разработаны модели, алгоритмы и методы МКА информационной безопасности исходного кода СиС на базе ТИВ на ОКИ, а также реализующий их программный прототип;
- созданы модели, алгоритмы и методы МКА информационной безопасности компонентного состава СиС на базе ТИВ на ОКИ, а также реализующий их программный прототип;
- сформулированы модели, алгоритмы и методы МКА информационной безопасности конфигурации СиС на базе ТИВ и их ресурсов на ОКИ, например, с использованием нейро-нечеткой идентификации аномалий [5];
- сделаны и апробированы модели, алгоритмы и методы МКА информационной безопасности ОКИ и их ресурсов, использующих ТИВ, по принципу «черного ящика», а также их программный прототип;
- спроектирована онтологическая модель данных для хранения информации о защищенности ОКИ, использующих ТИВ, а также реализующий ее программный прототип;
- разработан единый методологический подход к статическому МКА информационной безопасности СиС на базе ТИВ на ОКИ, объединяющий ранее упомянутые модели, алгоритмы и методы;
- созданы и проверены на практике модели, алгоритмы и методы формирования задач динамического МКА информационной безопасности СиС на базе ТИВ на ОКИ, на основе результатов статического анализа;
- разработан единый методологический подход к динамическому МКА информационной безопасности СиС на базе ТИВ на ОКИ, объединяющий ранее упомянутые модели, алгоритмы и методы;
- исследован и проработан единый методологический подход к комплексному МКА информационной безопасности СиС на базе ТИВ на ОКИ, в соответствии с подходами статического и динамического анализа
- создан программный прототип, реализующий систему комплексного МКА информационной безопасности СиС на базе ТИВ на ОКИ, использующий облачное хранилище данных.

Более того, в рамках решения задач МКА информационной безопасности СиС на базе ТИВ на ОКИ должны быть предложены научно-технические решения по применению на практике системы анализа.

Перечень решаемых вопросов и планируемых результатов позволяет говорить о том, что необходимо решить единую фундаментальную задачу, заключающуюся в разработке модельно-методологического аппарата, включающего совокупность взаимосвязанных моделей, алгоритмов и методов, а также программных прототипов, предназначенных для МКА информационной безопасности объектов критически важной инфраструктуры, использующих технологии Интернета вещей.

В рамках этой единой задачи необходимо не только объединить статические и динамические аспекты МКА информационной безопасности СИС Интернета вещей единым автоматизированным подходом с минимальным участием оператора, но и (например, за счет применения онтологической модели данных) сделать предлагаемые решения модульными, расширяемыми и иерархическими, а также способными работать в условиях недостатка или недоступности данных.

Таким образом, обоснованы этапы решения конкретных вопросов и сформулированы потенциальные результаты в рамках нового подхода к МКА информационной безопасности СИС на базе ТИВ на ОКИ. Данные вопросы могут и должны быть решены в интересах обнаружения слабых мест и архитектурных дефектов с точки зрения обеспечения защищенности подсистем такого класса.

Новый подход к МКА информационной безопасности СИС на базе ТИВ на ОКИ ориентирован на объединение направлений и алгоритмов статического и динамического контроля защищенности в рамках единого модельно-методологического аппарата.

Предложены пути и методологические комбинации для решения частных вопросов разработки моделей, алгоритмов и методов МКА информационной безопасности СИС на базе ТИВ на ОКИ, проанализированы возможности интеграции с другими системами.

*Исследование выполнено за счет гранта Российского научного фонда № 24-71-10095, <https://rscf.ru/project/24-71-10095/>, и Санкт-Петербургского научного фонда.*

#### СПИСОК ЛИТЕРАТУРЫ

1. Setola R., Luijff E., Theoharidou M. Critical Infrastructures, Protection and Resilience // Managing the Complexity of Critical Infrastructures / Studies in Systems, Decision and Control. Springer, 2016. pp. 1-18.
2. Верещагина Е.А., Капещкий И.О., Ярмонов А.С. Проблемы безопасности Интернета вещей. Учебное пособие М.: Мир науки, 2021 Сетевое издание. Режим доступа: <https://izd-mn.com/PDF/20MNNPU21.pdf> Загл. с экрана.
3. Котенко И.В., Парашук И.Б., Саенко И.Б. Информационная безопасность киберфизических систем: основные направления исследований // III-ая Межрегиональная научно-практическая конференция «Перспективные направления развития отечественных информационных технологий». Материалы конференции. Севастополь: СевГУ, 2017. С. 63-65.
4. Levshun D.S., Chechulin A.A. Vulnerability Categorization for Fast Multistep Attack Modelling // Proceedings of the 33rd Conference of the Open Innovations Association FRUCT. May 24-26, Zilina, Slovakia. 2023. pp. 169-175.
5. Fedorchenko E.V., Parashchuk I.B. Forecasting information security risks of critical infrastructures using neuro-fuzzy anomaly identification // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2024 (ICAIT-2024)). XIII Международная научно-техническая и научно-методическая конф.; сб. науч. ст. в 4 т. / Под. ред. С.А. Брусиловского. СПб.: СПбГУТ, 2024. Т. 1. С. 680-684.

УДК 004.056

#### РЕАЛИЗАЦИЯ УПРАВЛЕНИЯ КИБЕРБЕЗОПАСНОСТЬЮ СЕТИ ПЕРЕДАЧИ ДАННЫХ ЗА СЧЕТ СРЕДСТВ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ НА ОСНОВЕ МАШИННОГО ОБУЧЕНИЯ

Липатников Валерий Алексеевич<sup>1</sup>, Шевченко Александр Александрович<sup>2</sup>, Мелехов Кирилл Витальевич<sup>1</sup>

<sup>1</sup> Военная академия связи им. Маршала Советского Союза С. М. Буденного  
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

<sup>2</sup> Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевицкое пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mails: lipatnikovanl@mail.ru, alex\_pavel1991@mail.ru, kirill\_melehov@bk.ru

**Аннотация.** Жизненно необходимой мерой в современной цифровой среде является защита от кибератак, которые с каждым разом становятся все более сложными, целевыми и масштабными. Такая тенденция развития кибератак со стороны нарушителя требует принципиально новых подходов к защите сетей передачи данных. Поэтому разработка интеллектуальных средств поддержки принятия решений для управления кибербезопасностью является необходимым инструментом в борьбе с ними. Целью исследования является повышение эффективности средств поддержки принятия решений интеллектуальных систем управления кибербезопасностью сетей передачи данных. Результат: предложен алгоритм машинного обучения средств поддержки принятия решений интеллектуальных систем управления кибербезопасностью сетью передачи данных. Новизна: предлагаемые решения строятся на основе интеллектуальных технологий, позволяющим прогнозировать стратегии вторжения нарушителя. Практическая значимость: использование предложенного алгоритма позволит приступить к разработке средства поддержки принятия решений на основе машинного обучения для систем управления кибербезопасностью.

**Ключевые слова:** управление; кибербезопасность; сеть передачи данных; средства поддержки принятия решений; машинное обучение.

## IMPLEMENTATION OF CYBERSECURITY MANAGEMENT OF A DATA TRANSMISSION NETWORK USING MACHINE LEARNING-BASED DECISION SUPPORT TOOLS

Lipatnikov Valery<sup>1</sup>, Shevchenko Alexander<sup>2</sup>, Melekhov Kirill<sup>1</sup>

<sup>1</sup> Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny  
3 Tikhoretsky Av, St. Petersburg, 194064, Russia

<sup>2</sup> The Bonch-Bruевич Saint Petersburg State University of Telecommunications  
22 Bolshhevikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mails: lipatnikovanl@mail.ru, alex\_pavel1991@mail.ru, kirill\_melehov@bk.ru

**Abstract.** A vital measure in the modern digital environment is protection against cyber attacks, which are becoming more complex, targeted and large-scale every time. This trend in the development of cyber attacks by the intruder requires fundamentally new approaches to protecting data transmission networks. Therefore, the development of intelligent decision support tools for cybersecurity management is a necessary tool in the fight against them. The aim of the study is to increase the effectiveness of decision support tools for intelligent cybersecurity management systems for data transmission networks. Result: an algorithm for machine learning of decision support tools for intelligent cybersecurity management systems of a data transmission network is proposed. Novelty: the proposed solutions are based on intelligent technologies that make it possible to predict the intruder's invasion strategies. Practical significance: the use of the proposed algorithm will allow us to start developing a machine learning-based decision support tool for cybersecurity management systems.

**Keywords:** management; cybersecurity; data transmission network; decision support tools; machine learning.

Значимыми компонентом национальной безопасности в современных условиях являются сети передачи данных (СПД). Они, как и все цифровые систем уязвимы к кибератакам (КА) со стороны нарушителя. Для борьбы с КА необходимо внедрять и совершенствовать интеллектуальные систем управления кибербезопасностью (ИСУКБ), имеющих в своем составе средства поддержки принятия решений (СППР) способных, построенных на основе машинного обучения (МО) [1, 2].

В [3] предложен подход к проектированию системы автоматического оценивания эксплойтов, в основе которого лежит обучение модели для классификации исходных кодов эксплойтов по оценкам связанных уязвимостей методами глубокого обучения. В [4] рассматриваются вопросы выявления аномалий в сетевом трафике путем оценки его свойства самоподобия в реальном масштабе времени или близком к реальному, а обнаружение МЭА и их классификация осуществляются с применением гибридной нейронной сети, в основе построения которой базируются ячейки LSTM. В [5] разработана концепция интегрированной автоматизированной системы управления эксплуатацией автотранспорта, основанная на использовании комплекса интеллектуальных подсистем, включающих нейросетевые классификаторы, алгоритмы МО, элементы ИИ.

В связи с этим целью исследования является повышение эффективности средств поддержки принятия решений интеллектуальных систем управления кибербезопасностью сетей передачи данных.

Таким образом, в рамках поставленной задачи, для обеспечения возможности интеллектуальной автоматизации, удобства управления, мониторинга и проактивной защиты от вторжения нарушителя целесообразно создание моделей МО [6]. Предполагается, что этот процесс можно разбить на несколько ключевых шагов, каждый из которых играет важную роль в успешном функционировании модели.

Ниже представлены подробное описание ключевых шагов вышеуказанного процесса.

1. Начинается с определения задачи и постановки целей, где осуществляется: идентификация критических угроз, выбор типа задачи, критерии эффективности [7]. Реализуется моделирование атак на компоненты машинного обучения.

2. Далее, данные должны быть качественными и репрезентативными, такие как: источники данных, журналы безопасности. Определены основные данные для дальнейшего их использования при обучении модели, при этом они могут дополняться при необходимости.

3. После происходит подготовка данных, которые часто требуют очистки и предобработки, включая устранение пропусков, нормализацию, кодирование категориальных признаков и балансировку классов.

4. Одним из основных шагов является выбор подходящего алгоритма или модели, основываясь на характеристиках задачи, для аномалий, для прогнозирования и типе данных [8].

5. Следующим шагом реализуется обучение модели на основе подготовленных данных, что включает настройку параметров алгоритма и оптимизацию его работы [9]. Применяется **метод быстрого знака градиента** — техника состязательных атак в МО и глубоком обучении.

6. Затем выполняется валидация модели. После обучения необходимо оценить модель с использованием тестового набора данных для проверки ее производительности и способности к обобщению. Убедится в том, что модель действительно обучается правильным закономерностям, а не запоминает шум в данных. Без данного этапа невозможно построить надежную нейросеть.

7. Далее осуществляется настройка гиперпараметров. Всё определяется итогами оценки модели. Чтобы улучшить её работу может потребоваться оптимизация гиперпараметров.

8. На следующем шаге происходит развертывание модели. После достижения результатов модель готова к развертыванию в реальных условиях, что может подразумевать интеграцию с действующей системой.

9. После этого на заключительном шаге осуществляется мониторинг, обратная связь и обновление. Важно следить за ее производительностью в режиме «лайв». Необходимы периодические обновления модели, переобучая её на новых данных.

Разработка СППР для ИСУКБ СПД перестала быть опциональной задачей. Обеспечивается сокращение времени принятия решения путем изменения порогов в зависимости от наблюдаемого интервала времени [10]. Она является стратегической и обеспечивает устойчивость функционирования СПД к современным угрозам [11].

Системы управления кибербезопасностью должны быть **гибридными**. В таких системах МО должно их дополнять, а не заменять человеческую роль.

#### СПИСОК ЛИТЕРАТУРЫ

1. Липатников В.А., Мелехов К.В. Способ обработки результатов сетевого контроля при поддержке принятия решения администратора безопасности информации // Актуальные проблемы защиты и безопасности: Труды XXVII Всероссийской научно-практической конференции, Санкт-Петербург. Российская академия ракетных и артиллерийских наук, 2024. С. 306-310.
2. Гафаров Ф.М., Галимянов А.Ф. Искусственные нейронные сети и приложения: Учебное пособие. Издательство Казанского университета, 2018, 121 с.
3. Бусько Н.А., Федорченко Е.В., Котенко И.В. Автоматическое оценивание эксплойтов на основе методов глубокого обучения // Онтология проектирования. 2024. Т.14, №3(53). С. 408-420.
4. Котенко И.В., Саенко И.Б., Лаута О.С., Крибель А.М. Методика обнаружения аномалий и кибератак на основе интеграции методов фрактального анализа и машинного обучения // Информатика и автоматизация, 21(6). С.1328-1358.
5. Демьянчук С.В. Современные технологии и интеллектуальные системы в управлении эксплуатацией автотранспорта // Транспортное дело России. 2024. № 1. С. 245-248.
6. Котенко И.В., Саенко И.Б., Лаута О.С. [и др.] Атаки и методы защиты в системах машинного обучения: анализ современных исследований // Вопросы кибербезопасности. 2024. № 1(59). С. 24-37.
7. Липатников В.А., Мелехов К.В., Робак В.А., Шевченко А.А. Анализ уязвимостей и сетевых атак на ресурсы сетей передачи данных // Перспективы безопасности-2024: Сборник материалов II научно-технической конференции, посвященной информационной безопасности Санкт-Петербург: ООО «Специальный Технологический Центр», 2024. С. 29-37.
8. Свидетельство о государственной регистрации программы для ЭВМ № 2024681461 РФ. Программа обнаружения угроз безопасности сети передачи данных с использованием многослойной нейронной сети с обучением и минимизацией ошибок при сокращении времени сетевого контроля : № 2024661916 : заявл. 27.05.2024 : опубл. 10.09.2024 / Артамонов Н.М., Липатников В.А., Мелехов К.В. [и др.]. 02.05.2024 : опубл. 15.07.2024 / Абдрашитов М.С., Мелехов К.В., Липатников В.А. [и др.].
9. Свидетельство о государственной регистрации программы для ЭВМ № 2024666617 Российская Федерация. Программа обнаружения угроз безопасности сети передачи данных с использованием многослойной нейронной сети с обучением : № 2024619611 : заявл. 29.09.2023 : опубл. 11.02.2025 / Задбоев В.А., Липатников В.А., Мелехов К.В., Шевченко А.А. [и др.]; заявитель федеральное государственное казенное военное образовательное учреждение высшего образования «Военная академия связи имени Маршала Советского Союза С.М. Буденного» Министерства обороны Российской Федерации.
10. Липатников В.А., Шевченко А.А., Мелехов К.В. Метод повышения кибербезопасности масштабируемой критической информационной инфраструктуры путем многоуровневой интеллектуальной обработки данных для поддержки принятия решений по реагированию на инциденты безопасности // Прикладной искусственный интеллект: перспективы и риски : Сборник докладов Международной научной конференции, Санкт-Петербург, 17 октября 2024 года. СПб. : СПбГУАП, 2024. С. 414-416.
11. Патент № 2834591 С1 Российская Федерация, МПК G06F 21/50, G06F 21/60. Система контроля безопасности сети передачи данных: заявл. 29.09.2023 : опубл. 11.02.2025 / Задбоев В.А., Липатников В.А., Мелехов К.В., Шевченко А.А. [и др.]; заявитель федеральное государственное казенное военное образовательное учреждение высшего образования «Военная академия связи имени Маршала Советского Союза С.М. Буденного» Министерства обороны Российской Федерации.

УДК 621.396.4

#### **АНАЛИЗ ПОКАЗАТЕЛЕЙ БЕЗОПАСНОСТИ И РЕМОНТОПРИГОДНОСТИ ДАТА-ЦЕНТРОВ КАК ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ С ИСПОЛЬЗОВАНИЕМ ОНТОЛОГИЧЕСКОГО ПОДХОДА И МЕТОДОВ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ**

**Михайличенко Антон Валерьевич<sup>1</sup>, Михайличенко Николай Валерьевич<sup>2</sup>, Парашук Игорь Борисович<sup>1</sup>**

<sup>1</sup> Военная академия связи им. Маршала Советского Союза С. М. Буденного  
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

<sup>2</sup> Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича  
Большевикова пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mails: toni09\_91@mail.ru, 23esn2008@rambler.ru, shchuk@rambler.ru

**Аннотация.** В докладе рассмотрен новый методологический подход, нацеленных на формирование алгоритмов анализа показателей информационной безопасности и ремонтнопригодности дата-центров, как объектов критически важной инфокоммуникационной инфраструктуры, с использованием онтологий и иных современных способов интеллектуального анализа данных. Предложенный подход опирается на результаты решения задачи формирования уровней онтологии и частных метрик оценки безопасности и ремонтнопригодности, а также на поддержку своевременного принятия адекватных решений по восстановлению работоспособного состояния систем такого класса и гарантированному обеспечению их защищенности.

**Ключевые слова:** критическая инфокоммуникационная инфраструктура; дата-центр; безопасность; ремонтнопригодность; онтология; параметр; метрика; восстановление работоспособного состояния.

#### **ANALYSIS OF SECURITY AND MAINTENANCE INDICATORS OF DATA CENTERS AS OBJECTS OF CRITICAL INFOCOMMUNICATION INFRASTRUCTURE USING AN ONTOLOGICAL APPROACH AND METHODS OF INTELLIGENT DATA ANALYSIS**

**Mikhailichenko Anton<sup>1</sup>, Mikhailichenko Nikolay<sup>2</sup>, Parashchuk Igor<sup>1</sup>**

<sup>1</sup> The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny  
3 Tikhoretsky Av, St. Petersburg, 194064, Russia

<sup>2</sup> The Bonch-Bruevich Saint Petersburg State University of Telecommunications  
22 Bolshevikov Ave., bldg. 1, St. Petersburg, 193232, Russia  
e-mails: toni09\_91@mail.ru, 23esn2008@rambler.ru, shchuk@rambler.ru

**Abstract.** The report considers a new methodological approach aimed at forming algorithms for analyzing the indicators of information security and maintainability of data centers, as objects of critical information and communication infrastructure, using ontologies and other modern methods of intelligent data analysis. The proposed approach is based on the results of solving the problem of forming ontology levels and private metrics for assessing security and maintainability, as well as supporting timely adoption of adequate decisions on restoring the working state of systems of this class and guaranteed provision of their security.

**Keywords:** critical infocommunication infrastructure; data center; security; maintainability; ontology; parameter; metric; restoration of working condition.

В современных условиях вопросам обеспечения эффективной и безопасной работы дата-центров уделяется все больше внимания. Актуальность этой проблемы напрямую связана с необходимостью обеспечения их устойчивого функционирования в условиях перехода к «цифровой экономике», когда инфокоммуникации играют важнейшую роль [1–3].

Поэтому решение задачи повышения оперативности и достоверности анализа безопасности и ремонтпригодности (БиРП) дата-центров, как объектов критически важной инфокоммуникационной инфраструктуры, в интересах обнаружения в них «слабых» элементов (с точки зрения их защищенности и ремонтпригодности) и потенциальных угроз и технических дефектов, является актуальным. Основой защищенного и устойчивого функционирования дата-центров в условиях перехода к «цифровой экономике», является применение значимых количественных показателей их БиРП. Основной проблемой существующих показателей БиРП является их субъективность, в случае если речь идет об экспертных оценках критичности того или иного «слабого» элемента, того или иного потенциального технического дефекта. Более того, субъективность вносят и аспекты, связанные с отсутствием явной связи с уровнем безопасности и надежности дата-центров и механизма применения показателей защищенности и ремонтпригодности для определения данного уровня, например, уровня технической надежности в конкретном дата-центре [4].

В то время как современные средства мониторинга показателей защищенности и надежности предоставляют все больше подобной информации, старые подходы в области оценки БиРП, методы выбора мер их повышения уже не справляются с огромными объемами разнородных данных, с потоком данных об угрозах безопасности, авариях и отказах. Это подтверждается также ростом количества процедур импортозамещения, когда производители дата-центров не всегда могут использовать высоконадежные элементы. Все это предъявляет новые требования к анализу показателей БиРП дата-центров, как объектов критически важной инфокоммуникационной инфраструктуры, к анализу, ориентированному на выявление взаимосвязей между первичными данными по БиРП, метриками БиРП и уровнем общей защищенности и надежности систем такого класса. Считаем возможным решить эту задачу за счет определения природы информационно-телекоммуникационной инфраструктуры дата-центров, а также автоматизированного выявления обозначенных взаимосвязей, и разработки единого автоматизированного адаптивного механизма формирования и применения показателей БиРП в интересах их общей оценки и выбора мер их повышения с учетом условно неограниченного количества исходной информации. Суть предлагаемого подхода заключается в том, что в основу процесса оценки БиРП ставится набор иерархически взаимосвязанных метрик, позволяющих оценивать данные свойства инфраструктур подобных систем на разных этапах их функционирования и с разной степенью точности в зависимости от доступных данных о параметрах безопасности и сроках восстановления работоспособного состояния, новых знаний, получаемых в процессе оценки, и целей такой оценки.

Предполагается разработать онтологию показателей БиРП, ориентированную на задачи оценки данных свойств подобных систем и поддержки принятия решений по противодействию угрозам, вероятным авариям и отказам, методики обработки данных о БиРП на основе предлагаемой онтологии, методики расчета соответствующих показателей и методики применения онтологии в задачах оценки БиРП. Это позволит определить механизмы формирования обоснованных количественных метрик БиРП, привязанных к анализируемой системе, систематизировать накопленные в области метрик БиРП знания, определить методики их использования и расширения. Создание новых методов интеллектуального анализа данных о значениях параметров БиРП на основе онтологического подхода выведет системы управления дата-центров на качественно более высокий уровень, соответствующий подобным системам следующего поколения.

Анализ БиРП дата-центров предопределяет получение оценок нескольких ключевых параметров, например: вероятности вскрытия инфраструктуры, среднего времени взлома маршрутизатора, вероятности восстановления работоспособного состояния и других. Эти параметры могут лечь в основу методики анализа БиРП дата-центров, причем применение онтологического подхода совместно с интеллектуальным анализом данных обеспечит точность и оперативность оценки и выбора мер по восстановлению подобных систем, а также простоту дополнения новыми метриками, в случае появления новых данных.

Онтологический подход позволит построить систему метрик БиРП, состоящую из набора понятий и набора утверждений об этих понятиях, на основе которых можно строить классы, объекты, отношения, функции и теории, ориентированные на достоверный и оперативный анализ показателей БиРП дата-центров. При этом математический аппарат, положенный в основу онтологического подхода, позволяет ускорить время обработки данных о текущих значениях параметров защищенности и надежности систем такого класса [5].

От оперативности и достоверности решения задачи анализа БиРП дата-центров во многом зависит степень адекватности принимаемых, в конечном итоге, мер по заблаговременной подготовке средств защиты, ремонтной

базы и решений по интенсивности и очередности восстановления таких систем. Предложенный подход учитывает тот факт, что данная задача плохо подлежит строгой формализации, поэтому ее решение представляется возможным с использованием средств искусственного интеллекта, в частности, с использованием современных достижений в области представления и использования знаний. Поскольку из таких эффективных механизмов является концепция «онтологии», представляющая собой достаточно гибкий инструмент для описания объектов, классов, связей и атрибутов предметной области произвольной сложности, класс таких механизмов предложен для решения нашей задачи — анализа БиРП дата-центров, как объектов критически важной инфокоммуникационной инфраструктуры. Это обусловлено тем, что данный подход является актуальным в областях, где нужно хранить разнородную и быстро изменяемую информацию, например, текущие значения параметров БиРП, получаемые с датчиков в процессе мониторинга [6, 7].

Таким образом, рассмотрен ряд задач, нацеленных на формирование методики анализа показателей БиРП дата-центров, как объектов критически важной инфокоммуникационной инфраструктуры, с использованием онтологического подхода и современных методов интеллектуального анализа данных. Предложенный подход опирается на результаты решения задачи формирования онтологии и метрик оценки БиРП, а также на поддержку своевременного принятия адекватных решений по восстановлению работоспособного состояния систем такого класса и их защищенности.

#### СПИСОК ЛИТЕРАТУРЫ

1. Нагорный К.Д., Чеснов А.А., Чирков Т.А. Эксплуатация ЦОД: Практическое руководство. М.: Альпина ПРО, 2024. 320 с.
2. Прохоров А.Н., Рахматуллин С.С. Центры обработки данных. Анализ. Тренды. Мировой опыт. М.: АльянсПринт, 2021. 414 с.
3. Парашук И.Б., Михайличенко Н.В. Эффективность современных центров обработки данных // III Межрегиональная научно-практическая конференция «Перспективные направления развития отечественных информационных технологий». Материалы конференции, Севастополь: СевГУ, 2017. С. 24-26.
4. Боголепов Г.С., Михайличенко А.В., Парашук И.Б., Селезнев А.В. Оценивание и прогнозирование надежности мобильных дата-центров: математические модели смены состояний параметров безотказности, долговечности и ремонтпригодности // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. / Под. ред. А. В. Шестакова; сост. В. С. Елагин, Е. А. Аникевич. СПб.: СПбГУТ, 2022. Т. 3. С. 431-435.
5. Лутошкина Н.В. Модели знаний и онтологии. Красноярск: СибГУ им. М.Ф. Решетнева. 2021. 80 с.
6. Парашук И.Б., Крюкова Е.С., Михайличенко Н.В. Особенности и принципы оптимального адаптивного мониторинга центров обработки данных и электронных библиотек // Перспективные направления развития отечественных информационных технологий: материалы VI межрегиональной научно-практической конференции. Севастополь: СевГУ, Том2, 2020. С. 47-48.
7. Башкирцев С.А., Малофеев В.А., Парашук И.Б. Анализ роли и места задач мониторинга технического состояния в цикле управления системой связи и в процессе формулировки требований к автоматизированным системам управления связью // VI межвузовская научно-практическая конференция «Проблемы технического обеспечения войск в современных условиях». Труды конференции. СПб: ВАС, 2021. С. 136-140.

УДК 621.396.4

#### **ЗАЩИЩЕННОСТЬ МЕЖМАШИННОГО ИНФОРМАЦИОННОГО ОБМЕНА МЕЖДУ ЦЕНТРАМИ ОБРАБОТКИ ДАННЫХ: ПОДХОД К ГРУППИРОВКЕ ПРИЗНАКОВ УГРОЗ И ТИПОЛОГИЗАЦИИ РИСКОВ**

**Михайличенко Николай Валерьевич<sup>1</sup>, Парашук Игорь Борисович<sup>2</sup>**

<sup>1</sup> Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича  
Большевикова пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

<sup>2</sup> Военная академия связи им. Маршала Советского Союза С. М. Буденного  
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия  
e-mails: 23esn2008@rambler.ru, shchuk@rambler.ru

**Аннотация.** Доклад посвящен исследованию и обсуждению актуальные вопросов группировки признаков угроз и типологизации рисков информационной безопасности для процесса межмашинного информационного обмена между современными центрами обработки данных с использованием линий и каналов связи общего пользования. Рассмотрены сущность и содержание таких рисков с точки зрения угроз нарушения конфиденциальности, доступности и целостности информации, хранимой на центрах обработки данных, а также передаваемой по линиям и каналам связи общего пользования. Изучены и проанализированы внешние факторы, характеризующие физическое проявление рисков информационной безопасности для процесса межмашинного информационного обмена по линиям и каналам такого класса.

**Ключевые слова:** риски; угрозы; информационная безопасность; межмашинный обмен данными; линия связи общего пользования; признак; нарушение; центр обработки данных; канал.

#### **SECURITY OF MACHINE-TO-MACHINE INFORMATION EXCHANGE BETWEEN DATA CENTERS: AN APPROACH TO GROUPING THREAT SIGNS AND TYPOLOGIZING RISKS**

**Mikhailichenko Nikolay<sup>1</sup>, Parashchuk Igor<sup>2</sup>**

<sup>1</sup> The Bonch-Bruевич Saint Petersburg State University of Telecommunications  
22 Bolshhevikov Ave., bldg. 1, St. Petersburg, 193232, Russia

<sup>2</sup> Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny  
3 Tikhoretsky Av, St. Petersburg, 194064, Russia  
e-mails: 23esn2008@rambler.ru, shchuk@rambler.ru

**Abstract.** The report is devoted to the study and discussion of current issues of grouping threat attributes and typologizing information security risks for the process of machine-to-machine information exchange between modern data centers using public communication lines and channels. The essence and content of such risks are considered from the point of view of threats to the confidentiality, availability and integrity of information stored in data centers, as well as transmitted via public communication lines and channels. External factors characterizing the physical manifestation of information security risks for the process of machine-to-machine information exchange via lines and channels of this class are studied and analyzed.

**Keywords:** risks; threats; information security; machine-to-machine data exchange; public communication line; sign; violation; data center; channel.

Концепция межмашинного информационного обмена (МИО) между центрами обработки данных (ЦОД), использующего линии и каналы связи (ЛикС) общего пользования (ОП), представляют собой систему современных взглядов на процесс передачи и приема информации (документооборот) по таким ЛикС между территориально разнесенными автоматизированными техническими (аппаратно-программными) средствами и комплексами для хранения и обработки данных [1–5].

При этом самостоятельное и исключительно важное значение МИО между ЦОЦ по ЛикС ОП приобретает в современных условиях, когда подобные системы хранения и обработки данных все активнее используются в интересах органов административного управления регионального (например, областного), городского и муниципального уровней, где почти всегда и повсюду, должностные лица остро нуждаются в поливариантных защищенных информационных услугах, предоставляемых ЦОД [5, 6].

Вне всякого сомнения, и сам процесс МИО между ЦОЦ и вся информация (данные), создаваемая, хранящаяся, передаваемая и принимаемая по ЛикС ОП, уязвимы и чувствительны к рискам уничтожения и модификации, имеют насущную потребность в дополнительных манипуляциях (операциях в рамках политики безопасности), призванных гарантировать их защищенность. Причем, сегодня особого внимания и все большей заботы, с точки зрения обеспечения защищенности, заслуживает информация, непосредственно циркулирующая между ЦОД с использованием открытых ЛикС, а также внутри самих ЦОД, которые все активнее используются для эффективного функционирования киберфизических систем [7].

Ввиду этого, по нашему мнению, чрезвычайную важность приобретают анализ и группировка признаков угроз, а также типологизация рисков защищенности МИО между ЦОЦ по ЛикС ОП. При этом элементами процесса МИО между ЦОЦ, напрямую подверженными рискам информационной безопасности, являются не только и не столько сама информация (данные) и ее «носители», но и процедуры обработки этой информации в рамках систем такого класса, включая межмашинную передачу данных по линиям и каналам связи общего пользования. Небезызвестно, что признаки конкретных угроз и связанные с ними риски защищенности могут быть конвенционально сгруппированы по не наблюдаемым аспектам информационной безопасности МИО между ЦОЦ, причем эти риски, как и для иных потребителей, использующих ЛикС ОП, могут быть разделены по типам (типологизированы) на риски с позиции событий нарушения конфиденциальности, целостности и доступности информации, обрабатываемой и хранимой на ЦОД, а также принимаемой и передаваемой по линиям и каналам связи общего пользования, например, по каналам беспроводных сенсорных сетей [8].

В этом случае, в контексте признаков нарушения конфиденциальности, могут быть определены следующие типы явных и неявных рисков защищенности МИО между ЦОЦ по ЛикС ОП: нарушения конфиденциальности автоматизированного рабочего места (АРМ) системы МИО — риски непосредственного физического доступа к АРМ; нарушения конфиденциальности сервера операционной системы, на которой работает система МИО между ЦОЦ по ЛикС ОП — риски (угроза) загрузки на сервер вредоносного программного обеспечения; нарушения конфиденциальности сервера системы МИО между ЦОЦ — риски получения несанкционированного доступа напрямую к системе межмашинного обмена данными, в обход сервера операционной системы; нарушения конфиденциальности сервера базы данных адресов МИО — риски получения частичного или полного контроля над адресацией и маршрутизацией при межмашинном обмене; риски защищенности для ЛикС ОП, использующихся для межмашинного взаимодействия между ЦОД — угроза «перехвата» информации между ЦОД и серверами системы МИО; риски защищенности для ЛикС ОП, связанные с угрозой преднамеренной подмены маршрутов межмашинного обмена.

В рамках рассматриваемого подхода к группировке признаков угроз и типологизации рисков защищенности МИО между ЦОЦ по ЛикС ОП, аварийными (кризисными) событиями информационной безопасности подобного межмашинного взаимодействия в контексте признаков нарушения целостности, могут выступать риски, связанные с собственно информацией, участвующих в МИО: риски нарушения целостности данных, циркулирующих в рамках МИО (например, риски злонамеренной модификации данных); риски нарушения целостности (качества и вида) бэкап-файлов — резервных копий информации (данных), участвующей в МИО между ЦОЦ по ЛикС общего пользования [4].

Помимо прочего, риски защищенности МИО между ЦОЦ по ЛикС ОП могут быть, в общем виде, классифицированы по следующим типам: риски целостности межмашинного взаимодействия — связаны с угрозами уничтожения или искажения информации, которые могут быть как неумышленными, так и преднамеренными; риски конфиденциальности межмашинного взаимодействия — связаны с угрозами, при которых информация, предназначенная для межмашинного обмена, становится известна лицам, которые не должны иметь к ней доступа (перехват, кража информации), а также риски доступности межмашинного



взаимодействия — связаны с потенциальными угрозами, способными нарушить возможность получить своевременный и беспрепятственный доступ к информации пользователям и подсистемам ЦОД, имеющим все права доступа к ней.

Также риски защищенности МИО между ЦОЦ по ЛиКС ОП, в контексте выявления признаков нарушения доступности, могут быть сгруппированы по условиям реализации подобных нарушений: риски нарушения доступности, связанные с легкомысленным и нерадивым отношением к работе операторов межмашинного обмена, а также обусловленные невольными (ненамеренными) ошибками операторов и системных администраторов ЦОД, а также другого персонала, обеспечивающего межмашинное взаимодействие с использованием линий и каналов связи общего пользования [4].

Таким образом, исследованы и обсуждены актуальные вопросы группировки признаков угроз и типологизации рисков информационной безопасности для процесса МИО между современными ЦОЦ с использованием линий и каналов связи общего пользования. Рассмотрены сущность и содержание таких рисков с точки зрения угроз нарушения конфиденциальности, доступности и целостности информации, хранимой на ЦОД, а также передаваемой по ЛиКС ОП. Изучены и проанализированы внешние факторы, характеризующие физическое проявление рисков информационной безопасности для процесса межмашинного информационного обмена по линиям и каналам такого класса.

#### СПИСОК ЛИТЕРАТУРЫ

1. Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 27033-4-2021. Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 4. М.: Стандартинформ. 2021. 28 с.
2. Коржук В.М., Попов И.Ю., Воробьева А.А. Защищенный документооборот. Часть 1: Учебно-метод. пособие СПб.: Университет ИТМО, 2021. 67 с.
3. Вострцова Е.В. Основы информационной безопасности: учебное пособие. Екатеринбург: Изд-во Урал. ун-та, 2019. 204 с.
4. Милославская Н.Г., Толстой А.И. Управление рисками информационной безопасности. М.: Горячая Линия - Телеком. 2023. 224 с.
5. Парашук И.Б., Морозов И.В., Саяркин В.А. Подсистемы обеспечения безопасности электронного документооборота по каналам региональных телекоммуникационных сетей: требования и принципы построения // Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2022)». Санкт-Петербург, 26-28 октября 2022 г.: Материалы конференции. СПОИСУ. СПб.: 2022. С. 114-116.
6. Саяркин В.А., Домбровский Я.А., Парашук И.Б. Построение и оценка средств и комплексов защиты информации в современных системах обмена электронной корреспонденцией // Инновационная деятельность в Вооруженных Силах Российской Федерации: Труды всероссийской научно-практической конференции. 12-13 октября 2023 года, СПб.: ВАС, 2023. С. 607-612.
7. Парашук И.Б. Информационная безопасность телекоммуникационной компоненты киберфизических систем // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 4 / СПОИСУ. СПб.: 2017. С. 150-152.
8. Десницкий В.А., Парашук И.Б. Анализ и обеспечение защищенности данных пользователей беспроводных сенсорных сетей: показатели доступности, целостности и конфиденциальности // Региональная информатика и информационная безопасность. Сборник трудов. Вып. 7. СПОИСУ. СПб.: 2019. С. 34-38.

УДК 004.056

#### АНАЛИЗ БЕЗОПАСНОСТИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ ДЛЯ ЗАЩИЩЕННОЙ ПЕРЕДАЧИ ДАННЫХ

Николаева Полина Арсеновна

Военная академия связи им. Маршала Советского Союза С. М. Буденного  
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия  
e-mail: panicolaeva@mail.ru

**Аннотация.** Проведен анализ безопасности мобильных приложений для защищенной передачи данных. Рассмотрены основные угрозы, такие как MITM-атаки, уязвимости API, ошибки реализации протоколов шифрования и внедрение вредоносного кода. Особое внимание уделено анализу популярных мессенджеров, таких как Telegram и WhatsApp. Предложены практические рекомендации по улучшению архитектуры приложений, включая использование многофакторной аутентификации, шифрования данных и машинного обучения для обнаружения аномалий.

**Ключевые слова:** мобильные приложения; безопасность данных; криптография; машинное обучение.

#### ANALYSIS OF THE SECURITY OF MOBILE APPLICATIONS FOR SECURE DATA TRANSMISSION

Nikolaeva Polina

Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny  
3 Tikhoretsky Av, St. Petersburg, 194064, Russia  
e-mail: panicolaeva@mail.ru

**Abstract.** An analysis of the security of mobile applications for secure data transmission has been conducted. Key threats such as MITM attacks, API vulnerabilities, protocol implementation errors, and malicious code injection are considered. Special attention is paid to analyzing popular messengers like Telegram, and WhatsApp. Practical recommendations for improving application architecture are proposed, including the use of multi-factor authentication, data encryption, and machine learning for anomaly detection to enhance overall security.

**Keywords:** applications; data security; cryptography; machine learning.

Мобильные приложения активно используются для обмена конфиденциальными данными, такими как личная информация, банковские реквизиты и корпоративные данные. Однако их широкое распространение сопровождается ростом киберугроз [1]. Популярные мессенджеры, такие как Telegram и WhatsApp, применяют различные механизмы защиты данных, включая протоколы шифрования, аутентификации и управления ключами. Основные угрозы включают в себя MITM-атаки (перехват трафика), внедрение вредоносного кода через уязвимости в API, деобфускацию приложений и ошибки реализации протоколов. MTProto Telegram использует уникальные подходы к шифрованию, но критикуется за отсутствие полной прозрачности. WhatsApp, основанный на Signal Protocol, также демонстрирует высокий уровень безопасности, но уязвимости могут возникать на этапах управления ключами или взаимодействия с серверами [2]. Для повышения безопасности применяются многофакторная аутентификация, регулярное обновление библиотек безопасности и механизмы обнаружения аномалий. Машинное обучение помогает анализировать подозрительную активность в реальном времени. Сертификаты с жестким закреплением (certificate pinning) и усиленная верификация подлинности серверов снижают риски MITM-атак [3]. Технологии федеративного обучения позволяют анализировать данные без их централизации, что снижает вероятность утечек. Свёрточные автоэнкодеры и другие методы машинного обучения помогают обнаруживать аномалии в сетевом трафике и поведении пользователей. Современные подходы к защите данных включают использование искусственного интеллекта и гибридных технологий [4]. Например, защита голосовых каналов связи от подделок голоса становится важной задачей. Гибридные модели, такие как VAE-GAN, сочетают структурированное латентное пространство с высоким качеством генерации данных. Автоэнкодеры с пропускными связями позволяют строить более глубокие и стабильные сети. Комплексный подход, включающий биометрию, криптографию и машинное обучение, расширяет возможности защиты данных в мобильных приложениях [5, 6]. Современные разработчики стремятся сохранить баланс между удобством использования и надежностью.

#### СПИСОК ЛИТЕРАТУРЫ

1. Smith J., Johnson R. Mobile Application Security: Threats and Solutions // Journal of Cybersecurity. 2022. Vol. 8, № 3. P. 123–135.
2. Петров А.А., Сидоров В.В. Современные методы защиты данных в мобильных приложениях // Безопасность информационных технологий. 2021. № 4. С. 45–52.
3. Brown T., Lee K. Cryptographic Protocols in Messaging Apps: A Comparative Study // International Journal of Network Security. 2023. Vol. 15, № 2. P. 89–101.
4. Иванов Д.М. Анализ уязвимостей в API мобильных приложений // Программные продукты и системы. 2020. № 2. С. 78–86.
5. Wilson E., Davis M. Machine Learning for Anomaly Detection in Mobile Applications // Proceedings of the IEEE Conference on Security and Privacy. 2022. P. 234–245.
6. Zhang H., Liu Y. Enhancing Mobile App Security Through Advanced Cryptography // Journal of Information Security Research. Vol. 10, № 1. P. 56–68.

УДК 004.056

#### АНАЛИЗ БЕЗОПАСНОСТИ ОБЛАЧНЫХ СЕРВИСОВ И МЕТОДОВ ЗАЩИТЫ ДАННЫХ

Николаева Полина Арсеновна

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mail: panicolaeva@mail.ru

**Аннотация.** Облачные сервисы активно используются для хранения и обработки данных, но их безопасность требует особого внимания. Рассматриваются основные угрозы, такие как утечки данных через неправильные настройки, атаки на API, использование уязвимых приложений и недостатки в управлении доступом. Для защиты применяются современные методы, включая шифрование данных, многофакторную аутентификацию, системы обнаружения вторжений и постоянный мониторинг активности пользователей. Эти подходы помогают минимизировать риски и обеспечить надежную защиту информации.

**Ключевые слова:** облачные сервисы; защита данных; кибербезопасность.

#### ANALYSIS OF THE SECURITY OF CLOUD SERVICES AND DATA PROTECTION METHODS

Nikolaeva Polina

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mail: panicolaeva@mail.ru

**Abstract.** Cloud services are widely used for data storage and processing, but their security requires special attention. Key threats include data leaks due to misconfigurations, API attacks, vulnerabilities in third-party applications, and access management flaws. Modern protection methods such as data encryption, multi-factor authentication, intrusion detection systems, and continuous user activity monitoring are discussed. These approaches help minimize risks and ensure reliable information security in cloud environments.

**Keywords:** cloud services; data protection; cybersecurity.

Облачные сервисы активно используются для хранения и обработки данных, что делает их привлекательной мишенью для кибератак. Популярные платформы, такие как AWS, Microsoft Azure и Google

Cloud, предлагают различные механизмы защиты, но уязвимости всё равно возникают из-за ошибок конфигурации, недостатков в архитектуре или действий злоумышленников [1]. Основные угрозы включают несанкционированный доступ к данным, утечки через неправильно настроенные разрешения, атаки на API и использование уязвимых сторонних приложений. Например, данные могут быть скомпрометированы через открытые порты или слабые пароли. Для предотвращения таких инцидентов применяются строгие политики управления доступом, шифрование данных как в состоянии покоя, так и при передаче, а также постоянный мониторинг активности пользователей [2]. Шифрование данных играет ключевую роль в защите информации. Современные облачные сервисы поддерживают AES-256 для шифрования данных и TLS для безопасной передачи. Однако даже с этими технологиями важно регулярно обновлять ключи и сертификаты. Многофакторная аутентификация (MFA) помогает защитить учётные записи от взлома через фишинг или брутфорс [3]. Для повышения безопасности облачных сервисов применяются системы обнаружения вторжений (IDS) и системы предотвращения утечек данных (DLP). Эти технологии активно анализируют сетевой трафик, действия пользователей и события в системе, выявляя подозрительную активность. Например, IDS может обнаруживать аномалии в поведении пользователей, такие как необычные запросы к базам данных или попытки доступа к конфиденциальным файлам.

Системы DLP, в свою очередь, помогают предотвратить утечки данных за счет контроля передачи информации и применения политик безопасности. Также широко используются технологии искусственного интеллекта для анализа аномалий и прогнозирования потенциальных угроз, которые трудно обнаружить традиционными методами. Особое внимание уделяется защите данных в гибридных и мультиоблачных средах [4]. В таких системах данные распределены между несколькими провайдерами, что увеличивает риски из-за различий в политике безопасности и управлении доступом. Для минимизации этих рисков используются унифицированные системы управления политиками безопасности и инструменты для централизованного мониторинга. Контейнеризация и виртуализация также играют важную роль в защите облачных сервисов. Контейнеры, такие как Docker и Kubernetes, позволяют изолировать приложения и данные, снижая вероятность распространения атак. Кроме того, современные подходы к защите данных включают использование децентрализованных технологий, таких как блокчейн, для управления доступом и проверки целостности данных. Блокчейн обеспечивает прозрачность и неизменность записей, что особенно важно для защиты критически важной информации. Все эти методы дополняют друг друга, создавая многоуровневую систему защиты данных в облачных сервисах [5].

#### СПИСОК ЛИТЕРАТУРЫ

1. Smith J., Johnson R. Cloud Security Threats and Solutions // Journal of Cybersecurity. 2022. Vol. 8, № P. 123–135.
2. Петров А.А., Сидоров В.В. Современные методы защиты данных в облачных сервисах // Безопасность информационных технологий. 2021. № 4. С. 45–52.
3. Brown T., Lee K. Encryption Techniques in Cloud Computing: A Comparative Study // International Journal of Network Security. 2023. Vol. 15, № 2. P. 89–101.
4. Иванов Д.М. Анализ уязвимостей в облачных API // Программные продукты и системы. № 2. С. 78–86.
5. Wilson E., Davis M. Machine Learning for Anomaly Detection in Cloud Environments // Proceedings of the IEEE Conference on Security and Privacy. 2022. P. 234–245.

УДК 004.056

#### ЗАЩИТА ГОЛОСОВЫХ КАНАЛОВ СВЯЗИ ОТ DEEPFAKE АТАК

Николаева Полина Арсеновна

Военная академия связи им. Маршала Советского Союза С. М. Буденного  
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия  
e-mail: panicolaeva@mail.ru

**Аннотация.** Deepfake-технологии представляют серьезную угрозу для голосовых каналов связи, так как подделка голоса может использоваться для мошенничества, социальной инженерии и дезинформации. Рассматриваются методы обнаружения подделок, включая анализ спектральных характеристик, биометрическую аутентификацию и шифрование голосового трафика. Эти подходы помогают обеспечить защиту данных и повысить надежность голосовых систем связи.

**Ключевые слова:** голосовые каналы; deepfake; аутентификация; машинное обучение.

#### PROTECTION OF VOICE COMMUNICATION CHANNELS FROM DEEPFAKE ATTACKS

Nikolaeva Polina

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny  
3 Tikhoretsky Av, St. Petersburg, 194064, Russia  
e-mail: panicolaeva@mail.ru

**Abstract.** Deepfake technologies pose a significant threat to voice communication channels, as voice forgery can be used for fraud, social engineering, and misinformation. Methods for detecting fakes, including spectral analysis, biometric authentication, and voice traffic encryption, are discussed. These approaches ensure data protection and enhance the reliability of voice communication systems.

**Keywords:** voice channels; deepfake; authentication; machine learning.

Deepfake-технологии стремительно развиваются и становятся серьезной угрозой для голосовых каналов связи. Подделка голоса может использоваться для мошенничества, социальной инженерии или распространения дезинформации [1]. Современные генеративные модели, такие как WaveNet, Tacotron и GAN, способны создавать высококачественные подделки голоса с минимальными исходными данными — иногда достаточно всего нескольких секунд записи [2]. Это делает традиционные методы защиты уязвимыми и требует новых подходов. Поддельные голосовые сигналы создаются с помощью нейросетевых моделей, которые анализируют исходный голос и генерируют его копию. Эти модели могут имитировать не только тембр и интонацию, но и акцент, ритм речи и даже эмоциональную окраску. Для борьбы с такими атаками используются алгоритмы анализа спектральных характеристик голоса, выявление аномалий в сигнале и машинное обучение для классификации подлинности голоса. Системы аутентификации на основе биометрических данных помогают повысить надежность идентификации. Комбинирование голоса с поведенческими характеристиками, такими как ритм речи или акцент, значительно усложняет подделку. Также применяются методы шифрования голосового трафика для предотвращения перехвата данных злоумышленниками. Нейросетевые модели, обученные распознавать поддельные голосовые сигналы, эффективно обнаруживают deepfake в реальном времени. Системы мониторинга анализируют подозрительную активность и предупреждают о возможных атаках. Многофакторная аутентификация и регулярное обновление моделей машинного обучения позволяют адаптироваться к новым угрозам [3]. Гибридные подходы сочетают защиту голосовых каналов с анализом сетевого трафика. Например, внедрение технологий, таких как TLS и сертификаты с жестким закреплением (certificate pinning), помогает минимизировать риски перехвата данных. Шифрование голосового трафика и использование протоколов, защищающих данные от подмены, становятся стандартной практикой [4]. Комплексный подход, включающий биометрию, криптографию и машинное обучение, позволяет эффективно противостоять атакам deepfake. Защищенные голосовые системы находят применение в VoIP-приложениях, корпоративных коммуникациях и системах удаленной идентификации [5].

#### СПИСОК ЛИТЕРАТУРЫ

1. Goodfellow I., Pouget-Abadie J., Mirza M. et al. Generative Adversarial Nets // *Advances in Neural Information Processing Systems*. 2014. Vol. 27. P. 2672–2680.
2. Wang X., Lorenzo-Trueba J., Takaki S., Juvela L., Yamagishi J. Style Tokens: Unsupervised Style Modeling, Control and Transfer in End-to-End Speech Synthesis // *Proc. ICASSP*. 2022. P. 5989–5993.
3. Kinnunen T., Sahidullah M., Delgado H. et al. The ASVspoof 2019 Challenge: Future Horizons in Spoofed and Fake Audio Detection // *Proc. Interspeech*. 2021. P. 1023–1027.
4. Chen N., Qian Y., Lopez-Moreno I. et al. End-to-End Multimodal Authentication Against Replay Attacks // *IEEE Access*. 2022. Vol. 10. P. 45678–45690.
5. Jain A.K., Ross A., Prabhakar S. An Introduction to Biometric Recognition // *IEEE Transactions on Circuits and Systems for Video Technology*. 2020. Vol. 14. P. 4–20.

УДК 004.7

#### МЕТОДЫ МОНИТОРИНГА И ИДЕНТИФИКАЦИИ АНОМАЛЬНОГО ТРАФИКА В СЕТИ

**Ногин Сергей Борисович, Сычёв Кирилл Валерьевич, Емельяненко Артур Геннадьевич**

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: sprintnsb@mail.ru, sychev.kirill@gmail.com

**Аннотация.** В докладе рассматривается проблема роста сетевого трафика и его усложнения, что затрудняет анализ и повышает риски для сетевой безопасности. Особое внимание уделено аномальному трафику, который вызывает перегрузку сетевых ресурсов, снижает пропускную способность и нарушает нормальное функционирование сетевых сервисов. Анализируются современные методы мониторинга и выявления аномалий, включая нейронные сети, машинное и глубокое обучение. Рассмотрены основные источники аномального трафика, включая технические сбои и кибератаки, такие как DDoS, R2L, зондирование и U2R. Доклад подчеркивает важность разработки комплексных подходов к обнаружению аномалий для обеспечения устойчивости и безопасности сетевой инфраструктуры.

**Ключевые слова:** аномальный трафик; сетевая безопасность; мониторинг трафика; машинное обучение; DDoS-атаки; нейронные сети; киберугрозы; анализ трафика.

#### MONITORING IDENTIFICATION METHODS FOR ABNORMAL TRAFFIC ON THE NETWORK

**Nogin Sergey, Sychev Kirill, Emilianenko Artur**

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: sprintnsb@mail.ru, sychev.kirill@gmail.com

**Abstract.** This report examines the issue of increasing network traffic and its growing complexity, which complicates analysis and poses risks to network security. Special attention is given to abnormal traffic, which overloads network resources, reduces bandwidth, and disrupts normal network services. Modern methods for monitoring and detecting anomalies are analyzed, including neural networks, machine learning, and deep learning. The main sources of abnormal traffic are explored, covering both technical failures and cyberattacks such as DDoS, R2L, probing, and U2R.

The report emphasizes the importance of developing comprehensive approaches to anomaly detection to ensure network resilience and security.

**Keywords:** abnormal traffic; network security; traffic monitoring; machine learning; DDoS attacks; neural networks; cyber threats; traffic analysis.

С ростом популярности сети всё больше компаний и частных лиц сохраняют важные данные в интернете, что приводит к увеличению трафика в сети, но в то же время трафик становится более сложным, что усложняет его анализ. Аномальный трафик в сети занимает ресурсы пропускной способности, вызывает перегрузку и потребляет много памяти, ресурсов центрального процессора (ЦП) и т.д., из-за чего сеть не может предоставлять обычные услуги. Мониторинг и выявление аномального сетевого трафика — очень важная задача для обеспечения сетевой безопасности. Мониторинг и выявление аномального трафика в сети позволяют своевременно обнаруживать сбои и обеспечивать более эффективную передачу полезных пакетов, тем самым обеспечивая бесперебойную работу сети [1].

С развитием технологий для мониторинга и выявления аномального сетевого трафика стало применяться множество математических моделей. Благодаря исследованиям в области больших данных аномальный трафик отслеживается и идентифицируется с помощью нейронных сетей, машинного обучения, глубокого обучения и других методов.

Однако большинство современных исследований в области мониторинга и идентификации аномального трафика в сети сосредоточены на анализе одного метода и повышении производительности алгоритмов за счёт их улучшения, оптимизации и т.д.

Источники аномального трафика в сети можно разделить на два типа. Первый связан с самой сетью, например с нерациональной структурой сети, недоступностью оборудования и т.д. Второй тип связан с атаками на сеть, которые также являются объектом мониторинга и выявления аномального трафика. В настоящее время распространены следующие виды атак [2, 3].

1. Распределённая атака типа «отказ в обслуживании» (DDoS): распределённые крупномасштабные сетевые атаки, совершаемые несколькими злоумышленниками на один или несколько хостов, что приводит к их перегрузке и сбою. Это очень опасно.

2. Удаленный доступ к локальному (R2L): использование уязвимости системы для удаленного входа на хост и получения привилегий для выполнения некоторых незаконных операций.

3. Зондирование: сканирование IP-адреса, порта и т.д. цели и проведение целенаправленных атак на сеть.

4. User to Root (U2R): использование уязвимостей системы для получения доступа и кражи важной информации.

Рост сетевого трафика и его усложнение требуют эффективных методов мониторинга и выявления аномалий для обеспечения стабильной работы сетей [4]. Современные технологии, такие как машинное обучение и нейронные сети, позволяют автоматизировать процесс обнаружения угроз, однако большинство исследований фокусируются на отдельных методах, а не на комплексных решениях. Основными источниками аномального трафика являются как технические сбои, так и злонамеренные атаки, включая DDoS, R2L, зондирование и U2R. Для повышения сетевой безопасности необходимо дальнейшее развитие интеллектуальных систем анализа трафика, способных адаптироваться к новым видам угроз. Перспективным направлением является интеграция различных методов машинного обучения и создание гибридных систем для более точного и оперативного обнаружения аномалий.

#### СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 59547-2021. Национальный стандарт Российской Федерации. Защита информации. Мониторинг информационной безопасности. Общие положения» (утв. и введен в действие Приказом Росстандарта от 27.07.2021 N 656-ст) // [электронный ресурс]. URL: [https://e-ecolog.ru/docs/Fxw95Yk\\_uzl4rsalCAKLz/full?utm\\_referrer=https%3A%2F%2Fyandex.ru%2F/](https://e-ecolog.ru/docs/Fxw95Yk_uzl4rsalCAKLz/full?utm_referrer=https%3A%2F%2Fyandex.ru%2F/) (дата обращения 22.06.2025).
2. Как работает мониторинг компьютерных сетей // [электронный ресурс]. URL: <https://net-admin.ru/stati/kak-rabotaet-monitoring-kompyuternykh-setey/> (дата обращения 21.06.2025).
3. Методы мониторинга и обеспечения безопасности для поддержания работоспособности корпоративной сети // [электронный ресурс]. URL: <https://www.securitylab.ru/analytics/301808.php> / (дата обращения 21.03.2025).
4. Средства мониторинга и анализа // [электронный ресурс]. URL: [https://spravochnik.ru/informatika/sredstva\\_monitoringa\\_i\\_analiza\\_lokalnyh\\_setey/](https://spravochnik.ru/informatika/sredstva_monitoringa_i_analiza_lokalnyh_setey/) (дата обращения 23.06.2025).

УДК 004.7

#### К ВОПРОСУ МОНИТОРИНГА ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

Ногин Сергей Борисович, Сычёв Кирилл Валерьевич, Емельяненко Артур Геннадьевич

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: [sprintnsb@mail.ru](mailto:sprintnsb@mail.ru), [sychev.kirill@gmail.com](mailto:sychev.kirill@gmail.com)

**Аннотация.** В данной теме рассматриваются основы мониторинга компьютерной сети с точки зрения информационной безопасности РФ.

**Ключевые слова:** сетевой трафик; мониторинг; управление.

## ABOUT MONITORING THE LOCAL NETWORK

Nogin Syrgey, Sychev Kirill, Emelianenko Artur

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: sprintnsb@mail.ru, sychev.kirill@gmail.com

**Abstract.** In this topic, we will look at the basics of monitoring a computer network from the point of view of information security Russian Federation.

**Keywords:** network traffic; monitoring; management.

Для чего нужен мониторинг компьютерных сетей? Система мониторинга (СМ) компьютерных сетей является важным инструментом для обеспечения безопасности, стабильности и эффективной работы сети. Она должна отслеживать нестандартное поведение и возникновение исключительных ситуаций. Мониторинг сети позволяет выявлять подозрительную активность, вторжения и другие угрозы безопасности, что помогает оперативно реагировать и предотвращать атаки. Также позволяет отслеживать использование ресурсов сети, такие как пропускная способность, загрузка процессора и памяти, такое слежение помогает оптимизировать работу сети и предотвратить перегрузки.

На сегодняшний день в современные системы сетей внедряют уничтожить. Ну а если не удалось исправить исключительную ситуацию, то система сообщает о нарушении администратору сети. Таким образом, мониторинг компьютерных сетей на сегодняшний день играет ключевую роль в обеспечении безопасности, надежности и эффективности работы сети.

Как работает мониторинг компьютерных сетей? Мониторинг компьютерных сетей работает путем непрерывного отслеживания и анализа различных параметров сети, таких как пропускная способность, загрузка, задержка, ошибки и т.д. Это позволяет операторам сети быстро обнаруживать и устранять проблемы. В основном мониторинг компьютерных сетей делится на несколько задач:

1. Анализ — компания анализирует свою системную архитектуру, и ставит цели и задачи для СМ которые она должна решать.
2. Разработка — разработка платформы мониторинга, учитывается предыдущая ступень, учитываются возможные уязвимости, аппаратное обеспечение и так далее.
3. Запуск СМ — устанавливается и настраивается программное обеспечение, выделяются уязвимые узлы, в которых могут возникнуть неисправности.
4. Отслеживание — настройка основных мест, где возможно возникновение уязвимости.
5. Сбор и анализ — СМ собирает необходимые данные о работе сети, на основе полученных данных разрабатывается дальнейший план действий.

Средства мониторинга состояния сети:

1. Встроенные системы диагностики и управления.

Это программное обеспечение или аппаратные устройства, встроенные в сетевое оборудование, которые предназначены для мониторинга, диагностики и управления сетью. Эти системы обеспечивают возможность автоматического контроля и анализа состояния сети одного устройства, а также предоставляют

2. Системы управления сетью.

Network Management System — это система управления локальной сетью компании. Внедрение NMS систем в работу компании позволит постоянно контролировать работу всей локальной сети компании, особенно если в такой компании огромное количество устройств, подключенных к сети.

3. Средства управления системой.

System Management — выполняет функции учета аппаратных средств и внесения в базу данных, установкой ПО при помощи рассылки пакетов, удаленный анализ производительности сети, настройкой коммуникационного оборудования.

4. Анализаторы протоколов.

Protocol analyzers — это инструмент, который помогает отслеживать сетевой трафик и анализировать его поведение. Анализирует пакеты, отправленные по сети. Разделяется на 2 вида: аппаратный и программный, аппаратный может использовать как аппаратное, так и программное обеспечение для сбора и анализа пакетов. А программный только программное обеспечение для сбора и анализа.

5. Оборудование для диагностики и сертификации кабельных систем.

В основном делятся на четыре группы: сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры. Первый тип служит для тестирования кабелей различных категорий, а также собирает данные статистики трафика. Второй тип выполняют сертификацию на кабельные системы. Третий тип используются для диагностики медных кабельных систем. И последний четвертый тип, предназначены для проверки кабелей на отсутствие физического разрыва. В настоящее время есть более функциональные устройства, которые могут сочетать в себе несколько типов групп.

6. Экспертные системы. Такие системы собирают и накапливают знания технических специалистов о выявлении причин аномальной работы сетей, а также вариаций устранения неполадки. Такие системы в основном являются дополнением к основной системе.

7. Многофункциональные устройства анализа и диагностики. Такие устройства совмещают функции нескольких средств мониторинга.

Также компания при реализации различных средств мониторинга может обращаться к ГОСТУ “Р 59547-2021. Национальный стандарт Российской Федерации. Защита информации. Мониторинг информационной безопасности. Общие положения» (утв. и введен в действие Приказом Росстандарта от 27.07.2021 N 656-ст)” в котором по мимо общих сведений и требований к мониторингу информационной безопасности (ИБ) есть уровни мониторинга ИБ, которые помогают в реализации системы мониторинга. Выделяются следующие уровни мониторинга ИБ:

- уровень источников данных;
- уровень сбора данных;
- уровень хранения, агрегирования и обработки данных;
- уровень представления информации и данных мониторинга.

Таким образом, при помощи выбора нужных средств мониторинга и правильного разделения на уровни можно построить надежную систему в компании.

Организация безопасности сети при помощи средств мониторинга:

- мониторинг;
- мониторинг всей инфраструктуры;
- мониторинг пропускной способности сетевого канала;
- мониторинг сетевого трафика;
- мониторинг системных журналов;
- мониторинг безопасности устройств;
- мониторинг уязвимых точек;
- обнаружение и реагирование на инциденты.

Выше представлены одни из самых популярных мероприятий по обеспечению безопасности сети с помощью средств мониторинга. В каждом из параметров общий принцип работы заключается в необычные ситуации, которые могут потенциально угрожать безопасности сети.

Таким образом, можно сделать вывод, что разработанная системы мониторинга и управления сетью играют важную роль в обеспечении надежной и эффективной работы сети и позволяя оперативно реагировать на инциденты.

#### СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 59547-2021. Национальный стандарт Российской Федерации. Защита информации. Мониторинг информационной безопасности. Общие положения (утв. и введен в действие Приказом Росстандарта от 27.07.2021 N 656-ст) // [электронный ресурс]. URL: [https://e-ecolog.ru/docs/Fxw95Yk\\_uzl4rsalCAKLz/full?utm\\_referrer=https%3A%2F%2Fyandex.ru%2F/](https://e-ecolog.ru/docs/Fxw95Yk_uzl4rsalCAKLz/full?utm_referrer=https%3A%2F%2Fyandex.ru%2F/) (дата обращения 22.06.2025).
2. Как работает мониторинг компьютерных сетей // [электронный ресурс]. URL: <https://net-admin.ru/stati/kak-rabotaet-monitoring-kompyuternykh-setey/> (дата обращения 21.06.2025).
3. Методы мониторинга и обеспечения безопасности для поддержания работоспособности корпоративной сети // [электронный ресурс]. URL: <https://www.securitylab.ru/analytics/301808.php> / (дата обращения 21.03.2025).
4. Средства мониторинга и анализа // [электронный ресурс]. URL: [https://spravochnik.ru/informatika/sredstva\\_monitoringa\\_i\\_analiza\\_lokalnyh\\_setey/](https://spravochnik.ru/informatika/sredstva_monitoringa_i_analiza_lokalnyh_setey/) (дата обращения 23.06.2025).

УДК 004.942

#### ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ В УСЛОВИЯХ РАЗВИТИЯ ЦИФРОВЫХ ТЕЛЕКОММУНИКАЦИЙ И ТЕХНОЛОГИИ MACVIL

**Нуралинов Азамат Алдабергенович, Маликбаев Талгат Дусентаевич**

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: azamat.nur@mail.ru, tkarakesek@gmail.com

**Аннотация.** В данной работе рассматриваются ключевые аспекты информационной безопасности в условиях цифровизации и развития телекоммуникационных технологий. Особое внимание уделено военной сфере, где защита информации критически важна для оперативного управления войсками и успешного ведения боевых действий. Представлена технология MACVIL как перспективное решение для создания защищённых корпоративных и ведомственных сетей. Отмечены её преимущества в обеспечении высокой скорости передачи данных, устойчивости к внешним воздействиям и изоляции от публичной инфраструктуры. Технология рассматривается как основа построения безопасного информационного пространства в условиях современных киберугроз.

**Ключевые слова:** информационная безопасность; защита данных; MACVIL; профессиональная радиосвязь; телекоммуникационные технологии.

## INFORMATION SECURITY AND INFORMATION PROTECTION IN THE CONTEXT OF DEVELOPMENT OF DIGITAL TELECOMMUNICATIONS AND MACVIL TECHNOLOGY

Nuralinov Azamat, Malikbayev Talgat

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny  
3 Tikhoretsky Av, St. Petersburg, 194064, Russia  
e-mails: azamat.nur@mail.ru, tkarakesek@gmail.com

**Abstract.** This thesis explores key aspects of information security amid the digital transformation and the rapid development of telecommunications technologies. Special attention is given to the military sphere, where data protection is critical for effective troop command and combat success. The MACVIL technology is presented as a promising solution for creating secure corporate and departmental communication networks. Its advantages include high data transmission speed, resistance to external impacts, and independence from public infrastructure. MACVIL is considered a foundation for building a secure information environment in the face of modern cyber threats.

**Keywords:** information security; data protection; MACVIL; professional radio communication; telecommunication technologies.

В условиях стремительного развития цифровых технологий и повсеместного распространения информационно-коммуникационных систем вопросы защиты информации приобретают первостепенное значение.

Современное общество переживает цифровую трансформацию, при которой обмен, хранение и передача информации становятся основой как гражданских, так и военных процессов. Однако вместе с ростом объёмов данных и усложнением сетевой инфраструктуры возрастает и уязвимость информационных систем к внешним и внутренним угрозам.

Особое внимание следует уделять вопросам информационной безопасности в военной сфере, где передача и защита информации напрямую влияет на результат боевых операций, управление войсками и безопасность государства. В частности, в Десантно-штурмовых войсках Республики Казахстан информационная безопасность имеет решающее значение для поддержания устойчивой связи, координации действий в тылу противника и быстрого реагирования на угрозы [1].

Одной из перспективных технологий, обеспечивающих высокий уровень защищённости информации, является система профессиональной радиосвязи MACVIL (McWiLL). Она позволяет создать выделенные корпоративные и ведомственные сети с поддержкой не только голосовой связи, но и высокоскоростной передачи данных, видеонаблюдения, позиционирования и сервисов M2M/IoT.

Благодаря использованию смарт-антенн, адаптивной фильтрации полосы и высокой спектральной эффективности, технология обеспечивает устойчивую, защищённую и приоритетную связь даже в условиях высокой нагрузки или чрезвычайных ситуаций.

MACVIL значительно превосходит традиционные технологии (DMR, TETRA) по интеграции безопасности, скорости и функциональности.

В отличие от массовых сетей, которые легко поддаются перегрузке или могут быть отключены по решению операторов или властей, MACVIL работает независимо от публичной инфраструктуры, предоставляя гарантированный доступ и защищённость коммуникаций [2, 3].

Важнейшим аспектом применения технологии MACVIL является возможность изолированного управления потоками данных и предотвращения несанкционированного доступа к информации.

Системы MACVIL построены на принципах доверенного оборудования и отечественного ПО, что критически важно в контексте импортозамещения и обеспечения цифрового суверенитета [4].

Кроме военного применения, MACVIL активно внедряется в таких отраслях, как финансы, медицина, транспорт и энергетика, где защита информации также является приоритетом.

Благодаря гибкости и масштабируемости, технология способна адаптироваться под задачи любой сложности, сохраняя при этом ключевые параметры безопасности: конфиденциальность, целостность и доступность информации [5, 6].

Таким образом, технология MACVIL и развитие защищённых мультисервисных сетей связи становятся ключевыми элементами построения информационно безопасного пространства как в государственном, так и в корпоративном секторах. Их внедрение позволяет обеспечить устойчивость коммуникаций, защиту критически важной информации и готовность к противодействию современным киберугрозам.

### СПИСОК ЛИТЕРАТУРЫ

1. Электронная книга «Транкинговая система широкополосного доступа Маквил», А.Нуградинов.
2. Нуградинов А. Транкинговая система широкополосного доступа Маквил [Электронный ресурс]. URL: <https://www.livelib.ru/book/1149256/readpart-trankingovaya-sistema-shirokopolosnogo-dostupa-makvil-artut-nugradinov> (дата обращения: 25.08.2025).
3. Вооруженные силы [Электронный ресурс]. URL: [https://www.mod.gov.kz/rus/struktura/vooruzhennye\\_sily\\_rk/suxoputnye\\_voiska/struktura/?cid=31&rid=647](https://www.mod.gov.kz/rus/struktura/vooruzhennye_sily_rk/suxoputnye_voiska/struktura/?cid=31&rid=647) (дата обращения: 25.08.2025).
4. Д.Л. Шиллинг, Ф.Ф. Харрис. Основы телекоммуникационных систем. М.: Бином, 2005.
5. Научно-образовательный портал «Большая российская энциклопедия», Прокис, Дж. Цифровая связь. М.: Радио и связь, 2000.
6. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. М.: Вильямс, 2003.



УДК 621.396.4

# НЕКОТОРЫЕ АСПЕКТЫ БЕЗОПАСНОГО ПОИСКА ДАННЫХ НА РЕСУРСАХ ЕДИНОЙ СИСТЕМЫ ДАТА-ЦЕНТРОВ И ОБЛАЧНЫХ ХРАНИЛИЩ КАК КЛЮЧЕВОГО ЭЛЕМЕНТА ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ДОЛЖНОСТНЫХ ЛИЦ

Осадчий Александр Иванович<sup>1</sup>, Попков Юрий Алексеевич<sup>2</sup>, Носов Михаил Иванович<sup>3</sup>

<sup>1</sup> АО «Научный центр прикладной электродинамики»

Менделеевская ул., 8, литер А, помещ. 17 н, Санкт-Петербург, 194044, Россия

<sup>2</sup> Федеральное казенное учреждение «Войсковая часть 61535»

Хорошевское ш., 76 б, Москва, 123007, Россия

<sup>3</sup> Михайловская военная артиллерийская академия

Комсомола ул., 22, Санкт-Петербург, 195009, Россия

e-mails: ai\_osad@mail.ru, shchuk@rambler.ru, mikhail.nosov.64@mail.ru

**Аннотация.** Рассмотрены важные аспекты безопасного поиска данных должностными лицами различного уровня управления на ресурсах единой системы современных дата-центров и облачных хранилищ. Исследованы условия, которые могут повлиять на уровень защищенности процесса реализации поисковых запросов, как одного из важнейших процессов информационного обеспечения таких должностных лиц. Предложены некоторые формулировки для правил и механизмов обеспечения безопасного поиска на информационных ресурсах такого класса.

**Ключевые слова:** безопасность; поиск данных; ресурс; система; поисковый запрос; дата-центр; облачное хранилище; должностное лицо; информационное обеспечение.

## SOME ASPECTS OF SAFE DATA SEARCH ON THE RESOURCES OF A UNIFIED SYSTEM OF DATA CENTERS AND CLOUD STORAGE AS A KEY ELEMENT OF INFORMATION SUPPORT FOR OFFICIALS

Osadchiy Alexander<sup>1</sup>, Popkov Yuri<sup>2</sup>, Nosov Mikhail<sup>3</sup>

<sup>1</sup> Joint Stock Company "Scientific Center for Applied Electrodynamics"

8 Mendeleevskaya st., letter A, premises. 17 n, St. Petersburg, 194044, Russia

<sup>2</sup> Federal government institution "Military unit 61535"

76 b Khoroshevskoye sh., Moscow, 123007, Russia

<sup>3</sup> Mikhailovskaya Military Artillery Academy

22 Komsomola St., St. Petersburg, 195009, Russia

e-mails: ai\_osad@mail.ru, shchuk@rambler.ru, mikhail.nosov.64@mail.ru

**Abstract.** The article considers important aspects of secure data search by officials of various management levels on the resources of a single system of modern data centers and cloud storages. The article examines the conditions that can affect the level of security of the process of implementing search queries, as one of the most important processes of information support for such officials. Some formulations for the rules and mechanisms for ensuring secure search on information resources of this class are proposed.

**Keywords:** security; data retrieval; resource; system; search query; data center; cloud storage; official; information support.

Создание и совершенствование единой системы (ЕС) дата-центров (ДЦ) и облачных хранилищ (ОХ), представляющей собой программно-аппаратную платформу для информационного обеспечения должностных лиц органов управления в любой сфере жизнедеятельности государства, является актуальной, своевременной задачей. Речь о создании подобной единой системы для информационного обеспечения управленческой деятельности идет давно [1-3].

Это должна быть глобальная, доступная, гибкая, безопасная и мобильная платформа облачных вычислений и хранилища данных с зоной охвата всей территории России и ряда зарубежных территорий, а также тылового и оперативно-тактического пространства (с точки зрения обеспечения военной безопасности государства). Такая структура охватывает все ведомства и департаменты, отвечающие за жизнедеятельность и безопасность государства и призвана обеспечить хранение и обработку информации с использованием автоматизированной системы самообслуживания в рамках ЕС ДЦ и облачных вычислений с использованием последних достижений в области технологий обеспечения промышленной безопасности, ускоренной разработки и развертывания новых приложений и передовых компьютерных технологий. Одной из важнейших проблем, связанных с эффективным использованием ЕС ДЦ и ОХ, является проблема обеспечения оперативного и безопасного (защищенного) доступа должностных лиц к ресурсам такой платформы. Все это, по нашему мнению, обуславливает актуальность решения проблемы обеспечения безопасного (защищенного) доступа должностных лиц к ресурсам единой системы дата-центров и облачных хранилищ, являющейся ключевым элементом информационного обеспечения [4]. При этом частные задачи защищенной, своевременной и качественной реализации процедур доступа должностных лиц к ресурсам ЕС ДЦ и ОХ должны быть решены с учетом различных аспектов качества и безопасности, например [5-7]:

— должны быть, безусловно, выполнены правила политики безопасности в рамках всех возможных процедур оперативного поиска, компьютерных вычислений и хранения данных, причем с условием

гарантированной защищенности реализации этих возможностей в сложных условиях, в т.ч., в рамках проводимых масштабных бизнес-процессов и специальных операций силовых ведомств любого уровня;

- конфиденциальность, доступность и целостность искомых должностными лицами данных, должна быть обеспечена с учетом масштабируемости системы, с учетом возможности осуществлять поиск, вычисления и сохранять данные с высокой скоростью и гарантированной устойчивостью;

- безопасный поиск информации обеспечивается, опираясь на устойчивые сетевые возможности, соответствующие необходимости обработки больших массивов данных на глобальном уровне;

- должны быть учтены все аспекты безопасного поиска с учетом динамической масштабируемости и устойчивости на основе применения защищенных стандартных механизмов и протоколов;

- доступ должностных лиц к ресурсам ЕС ДЦ и ОХ должен обеспечиваться параллельно с мониторингом информационной безопасности этих ресурсов и происходящих событий, включая компьютерные атаки, сбои и замедление работы при использовании защищенного веб-интерфейса и программных интерфейсов установленных приложений, которые должны быть максимально безопасны в использовании;

- обеспечение возможности всем ведомствам и департаментам, отвечающим за жизнедеятельность и безопасность государства на всех их структурных уровнях контролировать безопасность поиска данных, конфиденциальность, доступность и целостность этих данных, а также защищенное взаимодействие с индивидуальными облачными сервисами ЕС ДЦ и ОХ;

- наличие механизма безопасного ролевого доступа к базам и хранилищам данных в рамках ЕС ДЦ и ОХ, в том числе административных органов и органов, отвечающих за политику безопасности, для обеспечения защищенного подключения новых облачных сервисов и управления существующими сервисами и службами;

- безопасный поиск информации на ресурсах ЕС ДЦ и ОХ должен быть ориентирован на поиск, облачные вычисления и хранение данных на основе стандартизированных, гарантированно безопасных аппаратно-программных конфигураций и политики безопасности, а также на основе стандартного механизма удаления любого программного компонента или службы поиска, в случае угрозы ее защищенности;

- информационный поиск и связанный с этой задачей защищенный доступ должностных лиц к ресурсам ЕС ДЦ и ОХ должны быть обеспечены механизмом для безопасной верификации должностного лица на основе современных протоколов удостоверения подлинности, включая многофакторное подтверждение аутентичности и инфраструктуры открытых ключей, которые будут работать на всех уровнях системы;

- при организации безопасного поиска данных на ресурсах ЕС ДЦ и ОХ должен быть обеспечен механизм объединения различных способов идентификации, включая использование временного интервала и индивидуальных устройств идентификации с сертифицированными параметрами ролевого доступа;

- должны быть учтены аспекты «сигнализации» и «персонификации» безопасного поиска с учетом наличия облачной службы оповещения о поиске конкретной информации конкретным должностным лицом (владельцем регистрационной записи на ресурсах ЕС ДЦ и ОХ);

- важно обеспечить возможность быстрого и безопасного размещения на ресурсах ЕС ДЦ и ОХ новых поисковых признаков и связанной с ними новой информации;

- и наконец, при организации безопасного поиска данных на ресурсах ЕС ДЦ и ОХ должно быть обеспечено ведение стандартных по форме и доступных по содержанию журналов аудита безопасности, т.е. журналов записи событий и инцидентов безопасности, происходящих при поиске конкретных данных на этих информационных ресурсах с целью отслеживания инициализации сервисов, изменений конфигурации, контроля доступа к службам и сервисам, ошибкам, а также любых иных событий безопасности.

Таким образом, рассмотрены важнейшие аспекты безопасного поиска данных должностными лицами различного уровня управления на ресурсах ЕС современных ДЦ и ОХ. Исследованы условия, которые могут повлиять на уровень защищенности процесса реализации поисковых запросов, как одного из важнейших процессов информационного обеспечения таких должностных лиц. Предложены некоторые формулировки для правил и механизмов обеспечения безопасного поиска на информационных ресурсах такого класса.

#### СПИСОК ЛИТЕРАТУРЫ

1. Костылева Н.В., Мальцева Ю.А., Шкурин Д.В. Информационное обеспечение управленческой деятельности: Учебное пособие. Екатеринбург: Изд-во Урал. ун-та, 2016. 148 с.
2. Крюкова Е.С., Паращук И.Б. Система показателей качества контента в рамках информационного обеспечения задач управления робототехническими комплексами военного назначения // Состояние и перспективы развития современной науки по направлению «Робототехника». Сборник статей V-ой научно-технической конференции. Изд-во ВИТ «ЭРА». Анапа, 2023. С. 107-117.
3. Башкирцев А.С., Малофеев В.А., Паращук И.Б. Формулировка современных требований к техническому и иным видам обеспечения автоматизированных систем специального назначения // V Межвузовская научно-практическая конференция «Проблемы технического обеспечения войск в современных условиях». Труды конференции. (20 марта 2020 г., г. Санкт-Петербург). СПб.: ВАС, 2020. С. 73-76.
4. Маковеев С.Н., Хорохорин О.А. Организация безопасного поиска информации в сети Интернет. Тамбов: Тамбовское областное государственное бюджетное учреждение «Компьютерный центр». 2015. 12 с.
5. Паращук И.Б., Царамов М.В., Сафонов Д.В. Анализ основных требований к процедурам поиска и навигации в больших объемах информации, циркулирующей в региональных телекоммуникационных сетях // Юбилейная XV-ая Санкт-Петербургская Международная конференция «Региональная информатика 2016 (РИ-2016)». Материалы конференции. СПб.: СПОИСУ, 2016. С. 114-115.
6. Котляшников И.А., Бырлова Е.А. Защита информации в «облачных технологиях» как предмет национальной безопасности // Молодой ученый. 2015. №6.4(86.4). С. 30-34.
7. Саяркин Л.А., Паращук И.Б., Владимиров Е.С. Этапы и особенности разработки методики повышения качества информационного поиска на ресурсах современных центров обработки данных с использованием нечетких отношений предпочтения и сравнения альтернатив // Информация и космос. № 1, 2024. С. 38-45.

УДК 004.056.2

# МОНИТОРИНГ РАБОТОСПОСОБНОСТИ ТЕЛЕФОННОЙ IP-СЕТИ И ОЦЕНКИ КАЧЕСТВА ПРЕДОСТАВЛЯЕМЫХ УСЛУГ С ПОМОЩЬЮ ПОГРАММНОГО МОДУЛЯ В УСЛОВИЯХ КИБЕРАТАК

Привалов Андрей Андреевич<sup>1</sup>, Титов Даниил Дмитриевич<sup>2</sup>, Боботина Полина Александровна<sup>3</sup>

<sup>1</sup> Академия войск национальной гвардии

Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия

<sup>2</sup>Петербургский государственный университет путей сообщения Императора Александра I,  
Московский пр-т., 9, Санкт-Петербург, 190031, Россия

<sup>3</sup>ОАО «Супертел»,

Петроградская наб., 38, Санкт-Петербург, 197101, Россия

e-mails: aprivalov@inbox.ru, titovdd178@gmail.com, titovdd178@gmail.com

**Аннотация.** Цель работы — создание программных средств для проактивного контроля защищённости IP-телефонных сетей и имитационного моделирования их работы в условиях кибератак с оценкой ключевых показателей качества обслуживания. В разработке применены математические и стохастические методы, включая графо-аналитические модели (сети GERT), вероятностный анализ и топологическое моделирование. Модель учитывает приоритетность трафика и поддерживает различные законы распределения (Парето, Вейбулла, гамма), что позволяет описывать самоподобный трафик с «тяжёлыми хвостами» по задержкам. Результаты подтверждают, что разработанные инструменты позволяют количественно оценить влияние различных кибератак (DDoS, комбинированные сценарии, сетевое сканирование) на время доставки пакетов, вероятность их потерь и время восстановления маршрутов, а также выявлять наиболее уязвимые элементы сети и оптимизировать стратегии маршрутизации. Практическая значимость состоит в том, что предлагаемые решения могут быть интегрированы в корпоративные и транспортные сети, обеспечивая упреждающий анализ устойчивости, сценарное моделирование последствий угроз и платформу для обучения персонала по сетевой безопасности.

**Ключевые слова:** IP-телефонная сеть; кибератака; надёжность сети; устойчивость сети; приоритетный трафик; имитационное моделирование; GERT; DDoS; сценарный анализ.

## MONITORING THE PERFORMANCE OF IP TELEPHONY NETWORKS AND EVALUATING THE QUALITY OF SERVICES PROVIDED USING A SOFTWARE MODULE IN THE CONTEXT OF CYBERATTACKS

Privolov Andrey<sup>1</sup>, Titov Daniil<sup>2</sup>, Bobotina Polina<sup>3</sup>

<sup>1</sup>Academy of the National Guard Troops

1 Pilot Pilyutova St, St. Petersburg, 198206, Russia

<sup>2</sup>Saint Petersburg State University of Transport,  
Moskovsky Prospekt, 9, Saint Petersburg, 190031, Russia

<sup>3</sup>Supertel OJSC

38 Petrogradskaya Emb, St. Petersburg, 197101, Russia

e-mails: aprivalov@inbox.ru, titovdd178@gmail.com, titovdd178@gmail.com

**Abstract.** The aim of the work is to create software tools for proactive control of the security of IP telephone networks and simulation modelling of their operation under cyberattack conditions with assessment of key quality of service indicators. Mathematical and stochastic methods are used in the development, including graph-analytical models (GERT networks), probability analysis, and topological modelling. The model takes into account traffic priority and supports various distribution laws (Pareto, Weibull, gamma), which allows describing self-similar traffic with 'heavy tails' in terms of delays. The results confirm that the developed tools allow for a quantitative assessment of the impact of various cyberattacks (DDoS, combined scenarios, network scanning) on packet delivery time, the probability of packet loss, and route recovery time, as well as identifying the most vulnerable elements of the network and optimising routing strategies. The practical significance is that the proposed solutions can be integrated into corporate and transport networks, providing proactive stability analysis, scenario modelling of threat consequences, and a platform for training personnel in network security.

**Keywords:** IP telephone network; cyberattack; network reliability; network resilience; priority traffic; simulation modelling; GERT; DDoS; scenario analysis.

Современные IP-телефонные сети всё чаще подвергаются целенаправленным кибератакам, способным дестабилизировать их работу. Распространённые угрозы включают распределённые атаки отказа в обслуживании (DDoS), перегрузку каналов связи, нарушения маршрутизации, атаки на протоколы сигнализации и аутентификации, сканирование и др. Такие атаки вызывают резкий рост задержек, деградацию качества обслуживания, потерю пакетов и сбои в работе узлов, вплоть до отказа критически важных сервисов. Особенно опасны они для сетей, обслуживающих транспорт, энергетику, медицину и другие важные объекты, где даже кратковременное нарушение связи может повлечь серьёзные материальные и социальные последствия.

Несмотря на актуальность проблемы, большинство средств мониторинга функционируют постфактум, не позволяя заранее оценить риски и спрогнозировать поведение сети при различных сценариях атак. Отсутствует также возможность безопасной проверки на действующей инфраструктуре. Таким образом, необходим проактивный подход к мониторингу, интегрированный с процессами управления инцидентами и обеспечивающий предварительный анализ устойчивости сети [1].

В данной работе предлагается комплексный инструмент, включающий программные модули для имитационного моделирования и оценки состояния IP-телефонной сети под воздействием кибератак. Применяется сочетание вероятностных и стохастических методов, таких как топологическое моделирование сети и графо-аналитические схемы GERT. Разработанная модель охватывает широкий диапазон факторов: интенсивность фоновой и вредоносного трафика, вероятности отказа узлов, динамическое изменение пропускной способности при перегрузках. Ключевой особенностью является поддержка различных распределений времени обслуживания и прибытия пакетов — помимо экспоненциального закона, используются распределения Вейбулла, Парето и гамма, что обеспечивает реалистичное описание самоподобного телетрафика с «тяжёлыми хвостами» распределения задержек. Кроме того, учитывается приоритетность сервисов: информационные потоки разделяются по категориям важности, влияющим на порядок обработки и ресурсы, выделяемые трафику при перегрузке. Предлагаемый подход интегрируется с процессами управления инцидентами, предоставляя средства для сценарного анализа «что, если» и поддержки принятия решений по кибербезопасности до наступления реальной атаки [2, 3].

Научная новизна:

1. Впервые для анализа устойчивости IP-телефонных сетей применён графо-аналитический аппарат GERT, позволяющий моделировать вероятностное прохождение трафика по альтернативным маршрутам и учитывать циклы повторной передачи пакетов при потерях.

2. Реализована гибкая поддержка различных законов распределения времени обслуживания и межпакетного интервала (гамма, Парето, Вейбулла), что повышает реалистичность имитационного моделирования по сравнению с классическими экспоненциальными моделями.

3. Введён механизм приоритетного обслуживания с разделением трафика на классы важности, позволяющий количественно оценить эффективность политики дифференцированного обслуживания (QoS) при атаках.

4. Смоделированы сложные комбинированные кибератаки (например, предварительная разведка сети с последующими DDoS-воздействиями), отражающие многофазный характер реальных угроз.

**Методология.** Математическая модель функционирования сети представляет собой дискретно-событийную имитацию, характеризуемую параметрами маршрутизации и обслуживания. Учитываются такие показатели, как среднее время восстановления маршрутов после отказов, пропускная способность каналов, интенсивности фоновой и атакующего трафика, ёмкость очередей и статистические свойства пакетов. Ключевые метрики качества обслуживания (время доставки, вероятность потерь, задержки) рассчитываются на основе формул с учётом выбранных законов распределения (Парето, Вейбулла, гамма). Для оценки надёжности сети используется коэффициент загрузки: при достижении критического значения, близкого к единице, система теряет устойчивость, и показатели качества резко ухудшаются [4].

Реализация модели выполнена посредством комбинации дискретно-событийного моделирования и метода Монте-Карло. Такой подход обеспечивает точное прогнозирование состояния сети при различных кибератаках и позволяет сравнивать альтернативные стратегии маршрутизации и защиты для выбора оптимальных мер.

**Результаты.** Серия экспериментов продемонстрировала эффективность разработанных модулей для количественного анализа последствий кибератак. При имитации DDoS-атак установлено, что сеть функционирует нормально при невысокой интенсивности вредоносного трафика, однако при превышении определённого порога ( $\rho \approx 1$ ) нагрузки вероятность своевременной доставки пакетов резко падает, очереди переполняются, и наступает фазовый переход к неустойчивому состоянию. Этот порог соответствует коэффициенту загрузки, близкому к 1, при котором происходит резкая деградация показателей качества обслуживания. Важным фактором является среднее время восстановления: более быстрое восстановление маршрутов после атак сокращает простой и повышает устойчивость системы.

Эксперименты с приоритетным обслуживанием (QoS) показали, что дифференциация трафика по классам позволяет поддерживать требуемое качество критически важных сервисов даже при высоком фоновом трафике или целенаправленной перегрузке. Высокоприоритетные потоки в условиях перегрузки продолжают обслуживаться с минимальными задержками, тогда как низкоприоритетные данные испытывают большие задержки и потери, что подтверждает эффективность механизмов QoS. В частности, временное отключение не критичного трафика на период атаки заметно улучшает показатели сети.

Отдельное внимание уделено сценариям комбинированных атак (например, скрытое сканирование сети перед массовой DDoS-атакой). Моделирование таких ситуаций позволило выявить наиболее уязвимые узлы и звенья, отказ которых приводит к максимальному ухудшению связности и качества. Заранее определив эти «точки отказа», можно усилить защиту на критических участках или внести изменения в маршрутизацию, повышая общую живучесть сети [5].

Предложенный проактивный подход к мониторингу и моделированию существенно расширяет возможности обеспечения устойчивости IP-телефонных сетей в условиях современных киберугроз. В отличие от традиционных методов пассивного мониторинга, ориентированных на регистрацию инцидентов постфактум,

разработанные решения дают возможность заранее проигрывать разнообразные сценарии атак и оптимизировать защитные меры до возникновения реальной угрозы. Объединение аналитических расчётов с имитационными экспериментами, учёт нетривиальных законов распределения телетрафика и приоритетного обслуживания позволили получить более точные прогнозы поведения сети под нагрузкой и обосновать эффективность защитных мер.

Практическая значимость подтверждается возможностью применения созданных модулей для повышения надёжности корпоративных, транспортных и иных критически важных сетей. Инструменты могут интегрироваться в существующие системы мониторинга и управления инцидентами, повышая эффективность реагирования. Они также могут использоваться как тренажёр для обучения персонала действиям в условиях кибератак. Перспективы включают автоматическую адаптацию модели к актуальным данным сети и использование методов машинного обучения для выявления новых типов атак и поддержки операторов при реагировании. Кроме того, планируется расширение набора сценариев атак и адаптация подхода для других типов сетей, что позволит создать универсальный инструмент обеспечения надёжности и безопасности сетевой инфраструктуры.

#### СПИСОК ЛИТЕРАТУРЫ

1. Privalov A., Kotenko I., Saenko I., Evglevskaya N., Titov D. Evaluating the functioning quality of data transmission networks in the context of cyberattacks // *Energies*. 2021. Vol. 14, No. 16. DOI: 10.3390/en14164755.
2. Lee J., Kim H., Park S. Security analysis of IP networks using Petri nets and Markov chains // *Journal of Network and Computer Applications*. 2020. Vol. 158. P. 102580. DOI: 10.1016/j.jnca.2020.102580.
3. Zhang Y., Li P., Wang X. Network intrusion detection based on deep learning algorithms // *Future Generation Computer Systems*. 2019. Vol. 93. P. 572–583. DOI: 10.1016/j.future.2018.10.039.
4. Иванов А. И., Колесников В. П. Моделирование приоритетного обслуживания трафика в сетях передачи данных при кибератаках // *Информационные технологии и вычислительные системы*. 2022. № 3. С. 45–52.
5. Васильев Д. Н., Соколов А. В., Семёнова Ю. А. Анализ перегрузок IP-сетей с использованием самоподобных моделей трафика // *Вестник связи*. 2021. № 4. С. 12–19.

УДК 621.396.4

#### ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ОБРАБОТКИ ДАННЫХ

**Ренсков Андрей Анатольевич, Ренсков Дмитрий Андреевич**

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий, пр., 3, Санкт-Петербург, 194064, Россия

e-mails: andreyrensko@gmail.com, dmitryirenskov@gmail.com

**Аннотация.** В условиях стремительного роста объёмов цифровой информации повышение эффективности обработки данных становится критически важной задачей для современных информационных систем. В статье рассматриваются перспективные направления, способствующие оптимизации процессов обработки больших объёмов разнородных данных. Проведён анализ современных подходов. Особое внимание уделено практическому применению перспективных направлений. Рассмотрены ключевые проблемы и ограничения, связанные с внедрением новых технологий. Сделан вывод о необходимости комплексного подхода к повышению эффективности обработки данных. Развитие перспективных направлений обработки данных способствует созданию более интеллектуальных, быстрых и безопасных информационных систем.

**Ключевые слова:** обработка данных; большие данные; искусственный интеллект; машинное обучение; облачные технологии; периферийные вычисления; распределённые системы; оптимизация алгоритмов.

#### PROMISING AREAS OF EFFICIENCY IMPROVEMENT DATA PROCESSING

**Renskov Andrey, Renskov Dmitry**

Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: andreyrensko@gmail.com, dmitryirenskov@gmail.com

**Abstract.** With the rapid growth of digital information, improving the efficiency of data processing is becoming a critical task for modern information systems. The article discusses promising areas that contribute to optimizing the processing of large amounts of heterogeneous data. The analysis of modern approaches is carried out. Special attention is paid to the practical application of promising areas. The key problems and limitations associated with the introduction of new technologies are considered. The conclusion is made about the need for an integrated approach to improving the efficiency of data processing. The development of promising areas of data processing contributes to the creation of more intelligent, faster and safer information systems.

**Keywords:** data processing; big data; artificial intelligence; machine learning; cloud technologies; peripheral computing; distributed systems; algorithm optimization.

В современном мире объёмы данных растут в геометрической прогрессии. Это делает обработку данных одной из ключевых задач в сфере информационных технологий, бизнеса, науки и государственного управления. Однако с ростом объёмов данных растут и требования к скорости их обработки, надёжности, безопасности и точности анализа.

Эффективная обработка данных позволяет организациям принимать более обоснованные решения, оптимизировать бизнес-процессы, выявлять закономерности и прогнозировать тенденции. В связи с этим особенно актуальным становится развитие новых технологий и методов, способных повысить эффективность обработки данных.

В работе рассматриваются перспективные направления повышения эффективности обработки данных, включая использование искусственного интеллекта, облачных технологий, распределённых вычислений, а также оптимизацию алгоритмов и архитектур обработки информации.

Современные информационные системы сталкиваются с необходимостью обработки больших объёмов разнородных данных в режиме реального времени, особенно в системах управления специального назначения. Это требует не только увеличения вычислительных мощностей, но и внедрения новых подходов к организации процессов обработки. Повышение эффективности обработки данных включает в себя как технические, так и алгоритмические аспекты, а также интеграцию инновационных решений в существующие архитектуры.

Одним из ключевых направлений является обработка больших данных. Такие технологии, как Apache Hadoop и Apache Spark, позволяют обрабатывать данные, объём которых превышает возможности традиционных СУБД. Распределённые системы обеспечивают высокую пропускную способность и отказоустойчивость.

В условиях непрерывного поступления данных особенно важной становится потоковая обработка. Такие платформы, как Apache Kafka и Apache Flink, обеспечивают обработку данных в режиме реального времени, что крайне важно для систем мониторинга, финансовых приложений и интернета вещей [1].

Искусственный интеллект и машинное обучение становятся неотъемлемой частью современных систем обработки данных. Алгоритмы машинного обучения позволяют автоматически выявлять закономерности, прогнозировать события и принимать решения без участия человека.

Облачные платформы (AWS, Google Cloud, Microsoft Azure) предоставляют масштабируемые ресурсы для обработки данных [2]. В свою очередь, периферийные вычисления позволяют обрабатывать данные ближе к источнику, сокращая задержки и нагрузку на центральные системы.

Разработка и внедрение более эффективных алгоритмов играют ключевую роль в повышении скорости обработки данных [3]. Это включает в себя: параллельные и асинхронные алгоритмы; использование графовых вычислений, применение квантовых алгоритмов (на ранних стадиях).

Архитектуры типа Data Lake позволяют хранить и обрабатывать структурированные и неструктурированные данные. Data Mesh — это более современный подход, основанный на децентрализации управления данными и распределении ответственности между доменами.

Интернет вещей генерирует огромные объёмы данных, требующих немедленной обработки. Интеграция Интернета вещей с системами обработки данных позволяет: оптимизировать производственные процессы; улучшить логистику и управление ресурсами; обеспечить безопасность и контроль.

Традиционные реляционные базы данных не всегда справляются с объёмами и скоростью поступления данных. Решения NoSQL (MongoDB, Cassandra) и NewSQL (CockroachDB, VoltDB) обеспечивают высокую производительность и гибкость.

Контейнеризация позволяет упростить развертывание и масштабирование приложений для обработки данных. Kubernetes обеспечивает автоматическое управление контейнерами, что повышает устойчивость и эффективность систем.

Для задач машинного обучения и анализа больших данных всё чаще используются графические процессоры (GPU) и специализированные чипы (TPU, FPGA), которые обеспечивают высокую вычислительную мощность.

Однако, существуют и проблемы: высокая стоимость; нехватка специалистов; проблемы обеспечения безопасности и конфиденциальности данных; сложность интеграции с устаревшими системами.

Примером практического применения перспективных направлений обработки данных является проект «Умный транспорт» в Москве. Система объединяет множество технологий для оптимизации городского транспортного потока, повышения безопасности дорожного движения и улучшения качества жизни горожан.

Используются технологии обработки больших данных (Big Data), Apache Kafka для сбора потоковых данных, Hadoop для хранения исторических данных, Spark для аналитики данных. Система собирает данные с более чем 200 000 видеокамер, 15 000 светофоров, GPS-навигаторов общественного транспорта и мобильных приложений пользователей. Ежедневно обрабатывается более 50 ТБ информации. В результате реализуется анализ транспортных потоков в режиме реального времени и прогнозирование пробок.

Алгоритмы машинного обучения анализируют поведение водителей, пешеходов и транспортных потоков, чтобы прогнозировать ситуацию на дорогах. Применяются: предиктивная аналитика для прогнозирования пробок за 30–60 минут; компьютерное зрение для распознавания нарушений ПДД; анализ моделей движения для оптимизации работы светофоров. Система обрабатывает потоковые данные с датчиков в режиме реального времени с задержкой менее 100 мс. Используемые технологии: Apache Storm, Apache Flink. При обнаружении ДТП система автоматически перенастраивает светофоры и информирует водителей через мобильное приложение.

Обработка данных происходит не только в центральных дата-центрах, но и на периферийных устройствах. Видеокамеры с ИИ-чипами самостоятельно распознают нарушения и отправляют только релевантные данные. В результате снижение нагрузки на сеть и уменьшение времени отклика. Все данные хранятся в едином хранилище, что позволяет проводить комплексный анализ. Используются технологии: Amazon S3, HDFS. В результате происходит интеграция данных из разных источников, гибкость аналитики.

Конкретные результаты внедрения: среднее время ожидания на светофорах сократилось на 25 %; автоматическое выявление 95 % нарушений ПДД; снижение количества ДТП с пострадавшими на 18 %; увеличение скорости реагирования на чрезвычайные ситуации на 40 %; сокращение времени ожидания на остановках на 20 %; сокращение времени простоя в пробках на 22 %.

Опыт Москвы успешно тиражируется в других городах России и за рубежом. Этот пример демонстрирует, как комплексное применение перспективных направлений обработки данных позволяет решать сложные городские задачи. Использование искусственного интеллекта, облачных технологий, новых архитектур и алгоритмов открывает широкие возможности для оптимизации бизнес-процессов и научных исследований.

Развитие перспективных направлений обработки данных будет способствовать созданию более интеллектуальных, быстрых и безопасных информационных систем, что, в свою очередь, окажет положительное влияние на развитие общества в целом.

#### СПИСОК ЛИТЕРАТУРЫ

1. Шапира Г., Палино Т., Сиварам Р., Петти К. Apache Kafka. Поточковая обработка и анализ данных, 2-е издание СПб.: Питер, 2024. 512 с.
2. Таненбаум Э. С., Бос Х. Современные операционные системы: СПб.: Питер, 2015. 1120 с.
3. Кнут Д. Э. Искусство программирования. Т. 1–4. М.: Диалектика-Вильямс, 2023. 3344 с.

УДК 621.396.4

### ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ И МЕТОДОВ КИБЕРБЕЗОПАСНОСТИ ДЛЯ ЗАЩИТЫ РЕГИОНАЛЬНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

**Ренсков Дмитрий Андреевич**

Военная академия связи им. Маршала Советского Союза С. М. Буденного  
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия  
e-mail: dmitryirenskov@gmail.com

**Аннотация.** В условиях цифровизации госуправления обеспечение кибербезопасности региональных информационных систем (РИС) становится ключевой задачей. В статье рассматриваются современные технологии для защиты критически важных систем: ИИ, Zero Trust, облачные решения, блокчейн и пост-квантовая криптография. Анализируются угрозы для российских РИС, включая децентрализацию и нехватку кадров. Особое внимание уделяется риск-ориентированному подходу, DevSecOps, управлению инцидентами и обучению персонала. Подчеркивается роль федеральных программ и межведомственного взаимодействия.

**Ключевые слова:** кибербезопасность; региональные информационные системы; модель «Никому не доверяй»; искусственный интеллект; критически важная информационная инфраструктура; управление рисками; цифровая трансформация; импортозамещение.

### THE USE OF MODERN CYBERSECURITY TECHNOLOGIES AND METHODS TO PROTECT REGIONAL INFORMATION SYSTEMS

**Renskov Dmitry**

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny  
3 Tikhoretsky Av, St. Petersburg, 194064, Russia  
e-mail: dmitryirenskov@gmail.com

**Abstract.** In the context of digitalization of public administration, ensuring the cybersecurity of regional information systems is becoming a key task. The article discusses modern technologies for protecting mission-critical systems: AI, Zero Trust, cloud solutions, blockchain, and post-quantum cryptography. The threats to Russian RIS, including decentralization and staff shortages, are analyzed. Special attention is paid to the risk-based approach, DevSecOps, incident management and staff training. The role of federal programs and interagency cooperation is emphasized.

**Keywords:** cybersecurity; regional information systems; Zero Trust; artificial intelligence; critical information infrastructure; risk management; digital transformation; import substitution.

В условиях стремительной цифровизации государственного управления, здравоохранения, образования, транспорта и других сфер жизнедеятельности региональные информационные системы становятся критически важными объектами инфраструктуры. Они хранят и обрабатывают персональные данные граждан, управляют бюджетами, обеспечивают функционирование муниципальных служб и взаимодействие между органами власти. В то же время растущая зависимость от цифровых платформ делает регионы всё более уязвимыми для кибератак — от массовых DDoS-атак до целенаправленного шпионажа и вымогательства данных.

Защита региональных информационных систем требует комплексного подхода, включающего не только технические меры, но и организационные, нормативно-правовые и кадровые аспекты. Современные технологии и методы кибербезопасности позволяют не только реагировать на угрозы, но и предотвращать их, обеспечивая устойчивость и доверие к цифровым сервисам на региональном уровне.

1. Особенности региональных информационных систем.

Региональные информационные системы (РИС) — это совокупность программно-аппаратных комплексов, используемых органами исполнительной власти субъектов РФ, муниципалитетами и подведомственными учреждениями для управления, сбора, обработки и хранения информации. К ним относятся:

- системы электронного правительства (порталы госуслуг, системы межведомственного взаимодействия);
- информационные системы здравоохранения (ЕМИАС, РМИС и др.);
- системы управления образованием (электронные дневники, системы приёма в вузы);
- системы ЖКХ, транспорта, экологии и социальной защиты.

Особенностью региональных информационных систем является их децентрализованная структура: каждый регион самостоятельно выбирает поставщиков, архитектуру и технологии, что приводит к фрагментации и разнородности систем. Кроме того, многие регионы сталкиваются с ограниченным бюджетом, нехваткой квалифицированных кадров и устаревшей инфраструктурой — всё это создаёт дополнительные риски.

Киберугрозы, с которыми сталкиваются РИС:

- DDoS-атаки направлены на выведение из строя порталов государственных услуг или систем здравоохранения;
- фишинг и социальная инженерия — используются для получения доступа к учётным записям сотрудников;
- программы-вымогатели (Ransomware) — шифруют данные и требуют выкуп, что особенно опасно для медицинских и образовательных учреждений;
- целевые атаки APT (Advanced Persistent Threat) — долгосрочные атаки, направленные на кражу конфиденциальной информации;
- уязвимости в программном обеспечении и оборудовании особенно опасны при использовании устаревших систем без регулярных обновлений.

## 2. Современные технологии кибербезопасности для защиты РИС.

Для эффективной защиты региональных систем необходимо внедрять комплекс современных технологий, адаптированных к специфике региональной инфраструктуры.

### 2.1 Искусственный интеллект и машинное обучение

ИИ и машинное обучение позволяют автоматизировать обнаружение аномалий и угроз в режиме реального времени. Системы на основе ИИ анализируют поведение пользователей, сетевой трафик, журналы событий и выявляют отклонения от нормы — например, нетипичные запросы к базе данных или попытки несанкционированного доступа. Это особенно важно для регионов, где не хватает специалистов по информационной безопасности.

Пример: платформы SIEM (Security Information and Event Management) с модулями машинного обучения, такие как IBM QRadar, Splunk Enterprise Security или отечественные решения «Ростелеком-СОЦ» и «Лаборатории Касперского».

### 2.2 Архитектура с нулевым доверием (ZTA).

Архитектура нулевого доверия предполагает, что ни одно устройство, пользователь или сеть не считаются доверенными по умолчанию — даже внутри периметра. Каждый запрос проходит многофакторную аутентификацию, авторизацию и проверку контекста (местоположение, устройство, время доступа).

Для региональных систем ZTA особенно актуальна, поскольку сотрудники часто работают удалённо, используя личные устройства, а границы сетей размыты. Внедрение ZTA снижает риск внутренних угроз и компрометации учётных записей.

### 2.3 Облачные решения и безопасность как услуга (SECaaS).

Многие регионы переходят на облачные платформы (например, ГосСУП, облачные решения «Ростелекома», «СберТеха»), что позволяет снизить затраты на инфраструктуру и получить доступ к современным средствам защиты. Модель SECaaS (безопасность как услуга) позволяет регионам использовать:

- облачные антивирусы и EDR/XDR-системы;
- системы защиты от DDoS-атак;
- управляемые центры управления безопасностью;
- платформы для управления уязвимостями и исправлениями.

Это особенно выгодно для малых и средних регионов, не имеющих собственных центров мониторинга безопасности.

### 2.4 Квантовая криптография и постквантовые алгоритмы.

Хотя квантовая криптография и постквантовые алгоритмы шифрования (например, разрабатываемые в рамках стандартизации NIST) пока не получили массового распространения, они уже сегодня рассматриваются как перспективное направление для защиты критически важных систем. Регионы, обрабатывающие особо важные данные (например, системы голосования, реестры граждан), могут начать подготовку к переходу на такие технологии.

### 2.5 Блокчейн для обеспечения целостности данных.

Блокчейн-технологии позволяют создавать неизменяемые реестры действий — например, журналы доступа, изменения в базах данных, результаты голосования. Это особенно полезно для систем, где важна прозрачность и невозможность подделки — например, в сфере земельного кадастра, распределения бюджетных средств или электронного голосования.

## 3. Методы и подходы к обеспечению кибербезопасности.

Технологии сами по себе не обеспечивают безопасность — необходима грамотная стратегия, основанная на лучших практиках и стандартах.



### 3.1 Принципы подхода, основанного на оценке рисков (RBA).

Подход, основанный на оценке рисков, предполагает определение приоритетности мер защиты в зависимости от критичности активов и вероятности угроз.

Для региона это означает:

- проведение регулярного аудита активов и выявление уязвимостей;
- классификацию данных по уровням конфиденциальности;
- сосредоточиться на защите наиболее важных систем (например, ЕГИСЗ, систем управления бюджетом).

### 3.2 DevSecOps и безопасная разработка

Многие региональные системы разрабатываются сторонними подрядчиками. Внедрение подхода DevSecOps (интеграция безопасности на всех этапах разработки) позволяет выявлять уязвимости ещё до запуска системы.

Это включает в себя:

- статический и динамический анализ кода (SAST/DAST);
- сканирование контейнеров и зависимостей;
- автоматизированное тестирование на проникновение.

### 3.3 Управление инцидентами и кибератаками.

В регионах должны быть отработанные планы реагирования на инциденты (IRP) и регулярно проводиться учения — как технические (например, имитация DDoS-атаки), так и командные (антикризисное управление). Участие в учениях «Киберполигон», организуемых ФСТЭК и Минцифрой, позволяет регионам отработать взаимодействие с федеральными центрами реагирования.

### 3.4 Обучение персонала к кибергигиены.

Человеческий фактор — одна из главных уязвимостей. Регулярное обучение сотрудников, тестирование на фишинг, внедрение политик кибергигиены (сложные пароли, двухфакторная аутентификация, запрет на использование личных устройств) значительно снижают риски.

4. Нормативно-правовая база и сотрудничество. В России действует комплексная нормативная база, регулирующая кибербезопасность региональных систем:

1. Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры»;
2. Приказы ФСТЭК России (например, № 21, № 31) по защите информации;
3. Национальная система сертификации средств защиты информации;
4. Указы президента и стратегии цифровой трансформации.

Регионы обязаны: классифицировать свои информационные системы; внедрять сертифицированные средства защиты; проводить аттестацию и лицензирование; взаимодействовать с Центром мониторинга и реагирования на компьютерные атаки (ЦМРКА) и НКЦКИ.

Кроме того, важно межрегиональное сотрудничество: обмен информацией об угрозах, совместные учения, унификация подходов. Создание межрегиональных центров управления безопасностью и центров компетенций позволяет эффективнее использовать ресурсы и опыт.

### 5. Перспективы и вызовы.

Несмотря на достигнутый прогресс, регионы сталкиваются с рядом проблем:

- Нехватка квалифицированных кадров. Решение — развитие региональных центров кибербезопасности при вузах, программы переподготовки, привлечение федеральных экспертов.
- Финансовые ограничения. Государственные программы субсидирования (например, через Минцифры и Фонд развития интернет-инициатив) могут частично компенсировать затраты.
- Быстрое развитие угроз. Требуется постоянное обновление технологий и методов — переход на автоматизированные системы, использование искусственного интеллекта, внедрение модели безопасности, ориентированной на угрозы (Threat Intelligence).
- Интеграция с федеральными системами. Необходима совместимость стандартов и протоколов, особенно при обмене данными с ЕСИА, ГИС ЖКХ, ЕГИСЗ и др.

Перспективными направлениями являются:

- создание региональных центров управления безопасностью с элементами искусственного интеллекта;
- внедрение цифровых двойников для моделирования атак и тестирования защиты;
- развитие кибериммунитета — архитектур, устойчивых к атакам по умолчанию;
- использование отечественных решений и импортозамещение в целях обеспечения технологического суверенитета.

Защита региональных информационных систем — это не просто техническая задача, а комплексный процесс, требующий стратегического подхода, инвестиций, подготовки кадров и постоянного совершенствования. Современные технологии — от искусственного интеллекта и модели «Никому не доверяй» до облачных сервисов SECaaS и блокчейна — предоставляют мощные инструменты для обеспечения устойчивости и безопасности. Однако их эффективность зависит от грамотной реализации, соответствия нормативным требованиям и вовлеченности всех участников — от рядовых сотрудников до руководителей регионов.

Для успешной цифровой трансформации регионов необходима надёжная защита от киберугроз. Только при обеспечении безопасности информационных систем можно гарантировать доверие граждан, эффективное управление и устойчивое развитие в цифровую эпоху.

#### СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
2. Стратегия национальной безопасности Российской Федерации (Указ Президента РФ № 683 от 31.12.2021).
3. Приказ ФСТЭК России № 21 «Об утверждении требований к защите информации...».
4. Отчет «Кибербезопасность в регионах России», АНО «Цифровая экономика», 2023.
5. Материалы конференции «Кибербезопасность регионов», Минцифры РФ, 2024.
6. Gartner. «Основные тенденции в области безопасности и управления рисками», 2024.
7. Специальная публикация NIST 800-207 «Архитектура нулевого доверия».

УДК 621.396.4

### ЗАДАЧИ, ЭТАПЫ И МЕТОДЫ ОБЕСПЕЧЕНИЯ АНАЛИЗА ЗАЩИЩЕННОСТИ ВЕДОМСТВЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ПРИ ИХ РАБОТЕ С СЕТЬЮ ОБЩЕГО ПОЛЬЗОВАНИЯ

**Рябов Геннадий Анатольевич, Паращук Игорь Борисович**

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: grif999@mail.ru, shchuk@rambler.ru

**Аннотация.** В докладе исследованы и обсуждены актуальные задачи, потенциальные этапы и возможные методы обеспечения анализа защищенности ведомственных телекоммуникационных сетей критически важных объектов при их работе с сетью общего пользования — глобальной телекоммуникационной сетью Интернет. Предложены конкретные методологические подходы к построению системы показателей качества функционирования средств и комплексов защиты информации для сетей такого класса. Изучены и проанализированы возможности использования для анализа защищенности унифицированных марковских моделей, а также методики и алгоритмов векторного динамического оценивания эффективности защиты информации.

**Ключевые слова:** ведомственная телекоммуникационная сеть; критически важный объект; сеть общего пользования; защищенность; анализ; эффективность средств и комплексов.

### TASKS, STAGES AND METHODS OF ENSURING SECURITY ANALYSIS OF DEPARTMENTAL TELECOMMUNICATION NETWORKS OF CRITICAL FACILITIES WHEN THEY WORK WITH A PUBLIC NETWORK

**Ryabov Gennady, Parashchuk Igor**

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: grif999@mail.ru, shchuk@rambler.ru

**Abstract.** The report examines and discusses current tasks, potential stages and possible methods for providing security analysis of departmental telecommunication networks of critical facilities when they work with the public network — the global telecommunication network Internet. Specific methodological approaches to building a system of performance indicators for information security tools and systems for networks of this class are proposed. The possibilities of using unified Markov models for security analysis, as well as methods and algorithms for vector dynamic assessment of information security effectiveness are studied and analyzed.

**Keywords:** departmental telecommunications network, critical facility, public network, security, analysis, efficiency of means and complexes.

Фундаментальная научная проблема, решение которой объективно назрело, заключается в разработке методологических основ обеспечения защищенности ведомственных телекоммуникационных сетей (ВТКС) критически важных объектов (КВО) при их работе с сетью общего пользования (СОП). В современных долговременных планах импортозамещения, развития и совершенствования значимых КВО страны большая роль отводится поиску путей решения проблемы повышения эффективности управления объектами такого класса и сложными технологическими процессами, реализуемыми ими.

С учетом интенсивных темпов развития современных социо-киберфизических систем и технологий, переходу на качественно новый уровень промышленной конкуренции, а иногда, и вооруженного противостояния, углубления процесса информатизации финансовых, производственных (например, промышленный Интернет вещей), политических и других действий, задача качественного управления КВО страны с наименьшими затратами приобретает приоритетное значение [1, 2].

Главенствующая роль проблемы эффективного управления значимыми для страны объектами и процессами для достижения успеха, подтверждается и опытом современных экономических, промышленных, политических и иных конфликтов. Одним из важнейших элементов развития страны, является создаваемое в

России Единое информационно-коммуникационное пространства (ЕИКП), которое объединит (организационно, информационно, структурно, функционально и территориально) все многообразие компьютерных сетей и ВТКС КВО страны — наиболее важных органов государственной власти, энергообеспечения, военно-промышленного комплекса, финансовых институтов и других КВО страны, и вместе с тем, реализует функции полномасштабного взаимодействия ВТКС КВО с сетью общего пользования — глобальной телекоммуникационной сетью Интернет.

Взаимоувязанная совокупность ВТКС КВО, являясь важным элементом ЕИКП, характеризуется реализацией общих и единых принципов построения, взаимосвязи, использования и защиты различных информационных и телекоммуникационных ресурсов КВО в целях достижения максимальной эффективности функционирования таких объектов, особенно при взаимодействии ВТКС КВО с сетью Интернет. Однако проблема обеспечения безопасности информации для ВТКС КВО при их работе с СОП, не просто является актуальной, а приобретает новые угрожающие аспекты. Особенно ярко это проявляется в области защиты от несанкционированного доступа (НСД) к ВТКС и контроля разграничения доступа к информационным и коммуникационным ресурсам ЕИКП. Общеизвестно, что информационная безопасность должна рассматриваться пользователями и задачами, решаемыми в рамках ВТКС КВО, не только с позиции конфиденциальности информации, но и с точки зрения комплексного обеспечения всех аспектов информационной безопасности, включая доступность и целостность информации. Это обусловлено тем, что разнородность ресурсов, используемых ВТКС КВО, предполагает наличие не только аппаратных, программных и информационных различий в области их построения и использования, но и различий в средствах и комплексах защиты информации (СКЗИ): в политиках безопасности, в применяемых механизмах защиты, в схемах разграничения доступа и т.д. Совместное использование ВТКС КВО этих ресурсов при их работе с СОП предполагает уточнение и доработку соответствующих политик безопасности и механизмов защиты, доработку процедур анализа защищенности и алгоритмов управления политикой безопасности, опирающихся на оценки уровня качества и эффективности системы защиты. А для их реализации необходима разработка соответствующего научно-методического обеспечения — математических моделей, методик и алгоритмов оценивания эффективности функционирования СКЗИ [3, 4].

Таким образом, проблема анализа эффективности защиты информации (ЗИ) в интересах обеспечения защищенности ведомственных телекоммуникационных сетей критически важных объектов при их работе с сетью общего пользования, должна рассматриваться как важнейшая проблема в области обеспечения не только безопасности этих ВТКС, обеспечения безопасности отдельных КВО, но и в области безопасности страны в целом, затрагивая при этом оборонную, социальную, экономическую, политическую, экологическую и другие составляющие. Обеспечение точного и оперативного анализа эффективности ЗИ, эффективности функционирования СКЗИ, обеспечение, на основе полученных оценок, защищенности ведомственных телекоммуникационных сетей критически важных объектов при их работе с сетью общего пользования, неразрывно связано с сохранением конфиденциальности информации КВО, ее целостности и доступности, что является необходимым условием дальнейшего эффективного развития экономики страны, ее оборонного комплекса, социальной сферы, науки и других сфер деятельности.

Цель дальнейших исследований в данном научном и практическом направлении, на наш взгляд, состоит в повышении точности и оперативности анализа эффективности функционирования СКЗИ в условиях различного вида воздействий на основе стохастического оценивания показателей качества систем защиты при взаимодействии ВТКС КВО с глобальной телекоммуникационной сетью Интернет. Основной задачей является: на основе анализа возможностей новых технологий ЗИ в современных и перспективных ВТКС КВО, теоретического обобщения существующих методов анализа качества СКЗИ в ВТКС, разработать математические модели, методику и алгоритмы векторного динамического оценивания эффективности функционирования СКЗИ при взаимодействии ВТКС КВО с СОП, учитывающие вероятностный и динамический характер процесса функционирования СКЗИ в условиях различного вида воздействий, включая алгоритмы теории катастроф [5].

Рассмотрим методы и подходы, с помощью которых планируется решение поставленных задач:

1. Разработка иерархической взаимоувязанной системы показателей качества (СПК) функционирования управляемых СКЗИ. Проведенный анализ различных методов формирования СПК сложных систем показал целесообразность использования, в качестве прототипа, подхода к формированию СПК, основанного на математических методах теории функциональной и параметрической декомпозиции.
2. Разработка математических моделей процесса функционирования СКЗИ на основе марковских цепей, учитывающих вероятностно-временной механизм изменения состояния показателей качества СКЗИ в динамике взаимодействия ВТКС КВО с глобальной телекоммуникационной сетью Интернет.
3. Оптимизация процесса анализа эффективности СКЗИ при взаимодействии ВТКС КВО с глобальной телекоммуникационной сетью Интернет. Для решения этой задачи предполагается разработать методику и алгоритмы векторного динамического оценивания эффективности защиты информации.

Таким образом, исследованы и обсуждены актуальные задачи, этапы и возможные методы обеспечения анализа защищенности ВТКС КВО при их работе с сетью общего пользования. Предложены конкретные методологические подходы к построению системы показателей качества функционирования средств и комплексов защиты информации для сетей такого класса. Изучены и проанализированы возможности использования для анализа защищенности унифицированных марковских моделей, а также методики и алгоритмы векторного динамического оценивания эффективности защиты информации.

## СПИСОК ЛИТЕРАТУРЫ

1. Вострецова Е.В. Основы информационной безопасности: учебное пособие для студентов вузов. Екатеринбург: Изд-во Урал. ун-та, 2019. 204 с.
2. Паращук И.Б. Информационная безопасность телекоммуникационной компоненты киберфизических систем // Региональная информатика и информационная безопасность. Сборник трудов. Вып. 4. СПОИСУ. СПб.: 2017. С. 150-152.
3. Милославская Н.Г., Толстой А.И. Управление рисками информационной безопасности. М.: Горячая Линия - Телеком. 2023. 224 с.
4. Паращук И.Б., Морозов И.В., Саяркин В.А. Подсистемы обеспечения безопасности электронного документооборота по каналам региональных телекоммуникационных сетей: требования и принципы построения // Региональная информатика (РИ-2022). Юбилейная XVIII СПб международная конференция «Региональная информатика (РИ-2022)». Санкт-Петербург, 26-28 октября 2022 г. : Материалы конференции. СПОИСУ. СПб.: 2022. С. 114-116.
5. Котенко И.В., Левшун Д.С., Паращук И.Б. Методы теории катастроф для задач оценки и прогнозирования уровня защищенности объектов критической инфраструктуры, использующих технологии Интернета вещей // Математические методы в технологиях и технике (ММТТ). 2025. № 1. С. 46-49.

УДК 004.056.5

**АНАЛИЗ ОБЩИХ И СПЕЦИАЛЬНЫХ ТРЕБОВАНИЙ К СИСТЕМЕ ОБНАРУЖЕНИЯ  
ВРЕДНОСНОЙ АКТИВНОСТИ В ТРАФИКЕ ИНФОКОММУНИКАЦИОННЫХ  
СЕТЕЙ И СИСТЕМ ИНДУСТРИАЛЬНОГО УМНОГО ГОРОДА**

**Саенко Игорь Борисович<sup>1</sup>, Котенко Игорь Витальевич<sup>1</sup>, Паращук Игорь Борисович<sup>1,2</sup>**

<sup>1</sup> СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия

<sup>2</sup> Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: ibsaen@comsec.spb.ru, ivkote@comsec.spb.ru, shchuk@rambler.ru

**Аннотация.** В докладе рассмотрены и сформулированы принципы, исследованы основные и дополнительные, функциональные и нефункциональные требования к системе обнаружения вредоносной активности в трафике инфокоммуникационных сетей и систем индустриального Умного города. Исследованы аспекты, учитывающие ключевые закономерности и базовые функции обнаружения вредоносной активности в инфраструктуре Умного города, а также условия применения новых интеллектуальных средств и методов для обнаружения подобной активности в инфраструктурах аналогичных киберфизических систем.

**Ключевые слова:** инфокоммуникационная сеть; система; требование; обнаружение вредоносной активности; принцип; функция; Умный город.

**ANALYSIS OF GENERAL AND SPECIFIC REQUIREMENTS TO THE SYSTEM FOR DETECTING  
MALICIOUS ACTIVITIES IN THE TRAFFIC OF INFOCOMMUNICATION NETWORKS  
AND SYSTEMS OF INDUSTRIAL SMART CITY**

**Saenko Igor<sup>1</sup>, Kotenko Igor<sup>1</sup>, Parashchuk Igor<sup>1,2</sup>**

<sup>1</sup> St. Petersburg Federal Research Center of the Russian Academy of Sciences

39, 14-th Linia, VI, St. Petersburg, 199178, Russia

<sup>2</sup> The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: ibsaen@comsec.spb.ru, ivkote@comsec.spb.ru, shchuk@rambler.ru

**Abstract.** The report examines and formulates principles, examines basic and additional, functional and non-functional requirements for the system for detecting malicious activity in the traffic of infocommunication networks and systems of the industrial Smart city. Aspects are examined that take into account key patterns and basic functions for detecting malicious activity in the infrastructure of the Smart city, as well as the conditions for using new intelligent tools and methods for detecting such activity in the infrastructures of similar cyber-physical systems.

**Keywords:** infocommunication network; system; requirement; detection of malicious activity; principle; function; Smart city.

Глобальная сеть Интернет и социальные сети стали одним из активнейших источников всевозможных угроз персональной, общественной и государственной информационной безопасности объектов и субъектов государства и киберфизических систем, например, таких, как индустриальный Умный город и входящие в него компоненты — Умный транспорт, Умное здравоохранение и т.п. [1–3].

Реализации различных угроз, так или иначе, предшествуют признаки, явно или косвенно указывающие на потенциальную возможность и нарастающую подозрительную тенденцию протекания сетевых инфокоммуникационных процессов, аномалии и «выбросы», нарушающие плавное и привычное течение сетевого трафика по каналам и трактам инфокоммуникационных сетей и систем индустриального Умного города. Такие признаки принято называть признаками вредоносной активности (ПВА) в трафике инфокоммуникационных сетей и систем [4, 5].

Поиск и идентификация ПВА происходят с помощью, так называемых, систем обнаружения вредоносной активности в сетевом трафике инфокоммуникационных сетей и систем индустриального Умного города. При этом очевидно, что система обнаружения вредоносной активности индустриального Умного города должна

осуществлять: регулярный мониторинг и обнаружение угроз в случае заражения вредоносным программным обеспечением; лучшую видимость угрозы и раннее обнаружение аномалий; проактивное предотвращение угроз и атак; безопасную передачу данных; обнаружение вредоносной активности следующего поколения для предотвращения атак вследствие уязвимостей; защиту серверов и приложений в центре обработки данных и в облаке, используемых в инфраструктуре Умного города и другие функции.

Исходными данными для формулировки требований к системе обнаружения вредоносной активности являются основные принципы и функции ее обнаружения в инфраструктуре Умного города, а также условия применения современных интеллектуальных систем для обнаружения такой активности в подобной современной инфраструктуре. Система обнаружения вредоносной активности в инфраструктуре индустриального Умного города выполняет несколько основных функций: ведет журнал вредоносной активности; выявляет вредоносную активность (признаки, аномалии, сигнатуры и атрибуты); выполняет функцию предупреждающей или онлайн сигнализации о появлении вредоносной активности (признаков, сигнатур, аномалий и атрибутов) для принятия решения администратором.

С учетом этого, базовыми принципами обнаружения ПВА принято считать: принцип признакового (сигнатурного, атрибутного) анализа и обнаружения: поиск соответствий какого-либо участка кода анализируемой (потенциально вредоносной) программы или событий известному коду (сигнатуре) или аномальным событиям из базы данных признаков, сигнатур и атрибутов вредоносной активности; принцип эвристического анализа и обнаружения: эмуляция работы анализируемой программы или воссоздание аномальных событий, создание журналов эмуляции и поиск соответствий данных из созданных журналов с данными из базы данных эмуляций (сигнатур) или базы данных аномальных событий, которые могут быть ПВА; принцип создания белых и черных списков признаков вредоносной активности: поиск вычисленной контрольной суммы от анализируемой, потенциально вредоносной, программы в базе данных контрольных сумм вредоносных программ, а также поиск и фиксация аномальных событий, которые могут быть признаками или атрибутами потенциальной вредоносной активности (чёрные списки) или в базе данных контрольных сумм легальных программ и не аномальных, типовых событий (белые списки); принцип проактивного анализа и обнаружения: предупреждающее обнаружение и перехват анализируемой, потенциально вредоносной, программы (или её частей) или аномальных событий; принцип ретроспективного анализа сетевой активности и поведения потенциально вредоносных программ.

С учетом этих основных принципов и функций систем обнаружения вредоносной активности в инфраструктуре Умного города, рассмотрим базовые и иные (функциональные и нефункциональные) требования к системам подобного класса, которые, на наш взгляд, должны включать:

Общие требования: требования к программным средствам системы обнаружения вредоносной активности в инфраструктуре индустриального Умного города; требования к аппаратным средствам — рабочим станциям и серверам (файловым серверам, серверам масштаба предприятия, терминальным серверам) системы обнаружения вредоносной активности в инфраструктуре индустриального Умного города; требования к программным и аппаратным средствам централизованного управления, мониторинга вредоносной активности и обновления на базе различных операционных систем; требования к обновлению баз данных контрольных сумм потенциально вредоносных программ, баз данных вызовов вредоносных программ, баз данных ПВА, а также баз данных эмуляций (сигнатур) и баз данных аномальных событий; требования к эксплуатационной документации систем обнаружения вредоносной активности в инфраструктуре Умного города; требования к технической поддержке систем обнаружения вредоносной активности.

Специальные (функциональные и нефункциональные) требования. В системах обнаружения вредоносной активности должны быть реализованы следующие специальные функциональные возможности: сканирование с целью поиска ПВА в режиме реального времени и по запросу из контекстного меню объекта инфраструктуры индустриального Умного города; эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные ПВА и вредоносные программы с целью нейтрализации действий активного вторжения и заражения; анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий; анализа вредоносной активности на ресурсах общих папок и файлов для выявления попыток шифрования защищаемых ресурсов доступных по сетям инфраструктуры индустриального Умного города; подготовка к блокировке действий вредоносных программ, которые используют уязвимости в программном обеспечении; подготовки и откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных вредоносными программами файлов; ограничения привилегий для процессов и приложений, динамически обновляемые настраиваемые списки приложений с определением уровня доверия с точки зрения вредоносной активности и иные.

Таким образом, исследованы и сформулированы принципы, обоснованы основные и дополнительные, функциональные и нефункциональные требования, которые учитывают ключевые принципы и базовые функции обнаружения вредоносной активности в инфраструктуре Умного города, а также условия применения новых интеллектуальных средств и методов для обнаружения вредоносной активности в подобных инфраструктурах.

*Исследование выполнено за счет гранта Санкт-Петербургского научного фонда № 23-РБ-01-09, <https://researchinspb.ru/news/40/>.*

#### СПИСОК ЛИТЕРАТУРЫ

1. Котенко И.В., Парашук И.Б. Анализ задач и потенциальных направлений разработки современных методов и средств обеспечения комплексной безопасности киберфизических систем типа «умный транспорт» // Научное обозрение. 2017. № 25, С. 26-30.

2. Василенко И.А., Василенко Е.В., Люлько А.Н. «Умный город» XXI века: возможности и риски смарт-технологий в городском ребрендинге. М.: Международные отношения, 2018. 256 с.
3. Парашук И.Б., Чечулин А.А. Нейро-нечеткий метод детектирования уязвимостей для контроля защищенности процессов и средств взаимодействия человек интеллектуальная система в рамках концепции «Smart Transport» // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2023). XII Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. / Под ред. С. И. Макаренко; сост. В.С. Елагин, Е.А. Аникевич. СПб.: СПбГУТ, 2023. Т. 1. С. 837-841.
4. Гольчевский Ю.В., Филимонова Н.А. Особенности некоторых аспектов информационной безопасности и обнаружение вредоносной активности в «Интернете вещей» // Нечеткие системы и мягкие вычисления. Промышленные применения (Ульяновск, 14–15 ноября 2017 г.) Материалы Первой всероссийской научно-практической конференции. Ульяновск: УГТУ. 2017. С. 56-66.
5. Parashchuk I.B., Doynikova E.V., Saenko I.B., Kotenko I.V. Selection of countermeasures against harmful information based on the assessment of semantic content of information objects in the conditions of uncertainty // 2020 International Conference on INnovations in Intelligent SysTems and Applications (INISTA). 24-26 Aug. 2020, Novi Sad, Serbia, 2020, IEEE Xplore Digital Library (11 September 2020). paper 24. pp.1-7.

УДК 621.391

## **ВАРИАНТ ПОВЫШЕНИЯ СКРЫТНОСТИ ПЕРЕДАЧИ ИНФОРМАЦИИ НА ОСНОВЕ ИЗМЕНЕНИЯ ХАОТИЧЕСКИХ СИГНАЛОВ-ПЕРЕНОСЧИКОВ**

**Сазонов Виктор Викторович, Альбадр Ходр Баракат**

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: vmktor-sazonov@yandex.ru, khodr.badr@gmail.com

**Аннотация.** Рассматриваются вопросы повышения скрытности передаваемой информации в помехоустойчивой хаотической системе передачи данных. Каждому биту ставится уникальная, циклически изменяемая, известная только на передающей и приёмной стороне доверенных пользователей, хаотическая реализация сигналов-переносчиков, с характерными им функциями автокорреляции. Используя положительные стороны уникальности структур хаотических сигналов-переносчиков и интегрального приёма, увеличивается помехоустойчивость и скрытность передаваемой информации.

**Ключевые слова:** скрытность передачи информации; помехоустойчивость; корреляционные функции хаотических сигналов-переносчиков; перезаписываемые накопители хаотических сигналов-переносчиков.

## **AN OPTION FOR IMPROVING THE STEALTH OF INFORMATION BASED ON CHANGING CHAOTIC CARRIER SIGNALS**

**Sazonov Viktor, Albadr Khodr**

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: vmktor-sazonov@yandex.ru, khodr.badr@gmail.com

**Abstract.** The issues of increasing the stealth of transmitted information in a noise-resistant chaotic data transmission system are considered. Each bit is assigned a unique, cyclically changing realization of a chaotic carrier signal, known only to the trusted users on the transmitting and receiving sides, characterized by their autocorrelation functions. By leveraging the uniqueness of the structures of chaotic carrier signals and integral reception, the noise resistance and stealth of the transmitted information are enhanced

**Keywords:** information concealment; noise immunity; correlation functions of chaotic carrier signals; rewritable storage devices for chaotic carrier signals.

Традиционные системы конфиденциальной связи [1–4] в тракте передачи данных используют псевдослучайные последовательности определённой длины, в основном построенные на основе кодов Баркера и М-последовательности. Основным недостатком таких систем является низкая защищённость псевдослучайных последовательностей, обусловленная современным состоянием когнитивного анализа их структур. В настоящее время, с учетом когнитивного характера возможного воздействия на системы передачи информации, для скрытия структуры передаваемых данных необходимо использовать хаотические сигналы-переносчики.

Однако следует отметить, что даже при «малой» интенсивности помех распознавание сигнала-переносчика, имеющего хаотическую структуру, может стать практически сложным, и как следствие реализация помехоустойчивой системы передачи информации, обладающей высокими показателями скрытности, затруднительна.

Самый простой способ повышения отношения сигнал/помеха заключается в увеличении мощности сигнала. Однако для этого приходится увеличивать мощность источника питания, а также габариты и вес всей аппаратуры передачи данных. Но, кроме повышения мощности сигнала, существуют и другие способы увеличения отношения сигнал/помеха. Например, использование на приёмной стороне одного из методов накопления, интегрального приёма или фильтрации.

В докладе рассматривается модифицированный вариант хаотической системы передачи информации. Он отличается от известной системы [5] двумя основными дополнениями: на передающей стороне добавлена возможность циклического изменения структуры хаотических сигналов-переносчиков (для этого используются настраиваемые линии задержки); на приёмной стороне добавлен вычислитель корреляционных функций хаотических сигналов-переносчиков.

Таким образом, используя положительные стороны интегрального приёма и циклического изменения хаотических сигналов-переносчиков, представляется возможным повысить помехоустойчивость и скрытность системы передачи информации.

#### СПИСОК ЛИТЕРАТУРЫ

1. Скляр, Бернард Цифровая связь. Теоретические основы практического применения. Изд. 2-е испр. Пер. с англ. М.: Издательский дом «Вильямс», 2003. 1104 с.
2. Семёнов А.М., Сикарев А.А. Широкополосная радиосвязь. Воениздат, 1970. 280 с.
3. Харкевич А.А. Основы радиотехники. 3-е изд., стер. М.: ФИЗМАТЛИТ, 2007. 512 с.
4. Максимов М.В. Защита от радиопомех. М. «Сов. радио», 1976. 496 с.
5. Баркетов С.В., Жук А.П., Сазонов В.В., Романько Д.В., Михайличенко Н.В., Шиянов А.В., Иванов А.С. Пат. 2369018 Российская Федерация, МПК Н04К 1/02. Система передачи информации хаотическими сигналами. Заявитель и патентообладатель Ставропольский военный институт связи ракетных войск. №2008116861/09 заявл. 28.04.08; опубл. 27.09.09, Бюл. №27. 9с: ил.

УДК 621.396.4

#### ИНТЕРФЕЙСЫ ДЛЯ РЕАЛИЗАЦИИ ПОИСКОВЫХ ЗАПРОСОВ: ФОРМУЛИРОВКА И ОБОСНОВАНИЕ МЕТРИК И СУБМЕТРИК ОЦЕНИВАНИЯ ЗАЩИЩЕННОСТИ

**Саяркин Леонид Андреевич, Паращук Игорь Борисович, Селезнев Андрей Васильевич**

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: leonid.sayarkin@yandex.ru, shchuk@rambler.ru, andrsel@mail.ru

**Аннотация.** В докладе рассмотрены этапы решения задачи обоснования и корректной математической формулировки вероятностной комплексной метрики и отдельных частных субметрик защищенности пользовательских интерфейсов для реализации поисковых запросов на ресурсах центров обработки данных. Разработанная вероятностная комплексная метрика призвана гарантировать точный текущий и прогнозный контроль уровня защищенности пользовательских интерфейсов для реализации поисковых запросов, она создана на базе обобщенной вероятности выполнения условий по отдельным частным субметрикам защищенности. Исследованы подходы к формулировке частных субметрик защищенности интерфейсов, изучены перспективные направления для создания на их основе алгоритмов точного и своевременного контроля информационной безопасности объектов такого класса.

**Ключевые слова:** реализация поисковых запросов; метрика; защищенность; интерфейс; информация; оценивание; требования; условная вероятность; целостность; доступность; конфиденциальность.

#### INTERFACES FOR IMPLEMENTING SEARCH QUERY: FORMULATION AND JUSTIFICATION OF SECURITY ASSESSMENT METRICS AND SUBMETRICS

**Sayarkin Leonid, Parashchuk Igor, Seleznev Andrey**

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: leonid.sayarkin@yandex.ru, shchuk@rambler.ru, andrsel@mail.ru

**Abstract.** The report considers the stages of solving the problem of substantiation and correct mathematical formulation of a probabilistic complex metric and individual private submetrics of user interface security for implementing search queries on data center resources. The developed probabilistic complex metric is designed to guarantee accurate current and predictive control of the level of user interface security for implementing search queries; it is created on the basis of a generalized probability of fulfilling conditions for individual private submetrics of security. Approaches to formulating private submetrics of interface security are investigated, promising directions for creating algorithms for accurate and timely control of information security of objects of this class on their basis are studied.

**Keywords:** search query implementation, metric, security, interface, information, evaluation, requirements, conditional probability, integrity, availability, confidentiality.

Аналитические и поисковые средства реализации запросов пользователей на получение конкретной релевантной информации на ресурсах современных центров обработки данных (ЦОД), аппаратные и программные пользовательские интерфейсы для информационного поиска, не вполне удовлетворяют требованиям по защищенности процедур поиска.

Актуальность и значимость задач контроля и обеспечения защищенности программно-аппаратных интерфейсов информационного поиска на цифровых ресурсах ЦОД не только выходят на первый план, но и занимают главенствующие позиции при формулировке технических заданий на создание и построение таких систем информационного обеспечения, которые представляют собой согласованные по времени и задачам стационарные либо мобильные взаимосвязанные комплексы организационных и программно-аппаратных средств, предназначенных для создания высокопроизводительной и отказоустойчивой инфраструктуры, отвечающей за обработку, хранение и выдачу информации.

В частности, речь идет о проблемах, связанных со слабой защищенностью человеко-машинных интерфейсов для реализации поисковых запросов (ИРПЗ) на цифровых ресурсах объектов такого класса, а также недостаточной полнотой и точностью предоставляемых из большого массива данных по конкретному запросу

пользователя за интервал времени. Сложность сравнительной многофакторной вероятностно-временной оценки защищенности таких программных и аппаратных информационно-технических средств взаимодействия пользователя и поискового механизма, каким и являются ИРПЗ, связана с тем, что в соответствии с одними метриками более защищенным может оказаться один ИРПЗ, а в соответствии с другими метриками — совсем другой программно-аппаратный интерфейс для реализации поисковых запросов [1, 2].

Известен и достаточно подробно изучен ряд зарубежных и национальных стандартов, определяющих методологические подходы к анализу защищенности объектов такого класса и примерный перечень метрик, в соответствии с которыми она могут быть оценена в целом. Но чаще всего оцениваются такие аспекты (субметрики) защищенности интерфейсов, как доступность, конфиденциальность и целостность данных для поиска, передачи, приема и обработки, для чего, собственно, и служат ИРПЗ.

Кроме того, приходится также учитывать субъективизм формулировки некоторых отдельных частных субметрик защищенности (ЧСМЗ) ИРПЗ, вносящий известную либо неизвестную, но существенную, долю неопределенности в решение задач вероятностно-временного оценивания доступности, конфиденциальности и целостности интерфейсов такого класса [3, 4].

Приемлемый вариант решения этой проблемы, на наш взгляд, может быть получен в рамках формулировки и последующей текущей либо прогностической оценки данного важного свойства — безопасности, на основе вероятностной комплексной метрики защищенности (ВКМЗ) ИРПЗ, которая бы функционально связывала все многообразие ЧСМЗ и требований к ним [5].

Детальное исследование существующих разнообразных подходов к формированию комплексных (обобщенных) метрик качества, эффективности, либо безопасности сложных технических систем, показало, что в наибольшей степени учет особенностей решения задачи оценивания защищенности интерфейсов взаимодействия при решении задач информационного поиска, а также элементарное решение математической задачи нормализации и свертки метрик защищенности (МЗ) может быть достигнуто при использовании вероятностной скаляризации.

Идея данного метода состоит в использовании в качестве ВКМЗ совместной вероятности выполнения условий (требований) по отдельным частным субметрикам защищенности ИРПЗ на конкретном шаге реализации поисковых запросов, частным субметрикам по доступности, конфиденциальности и целостности.

Безусловное достоинство данного метода связано с учетом случайного характера изменений подавляющего большинства МЗ ИРПЗ, а также практической возможностью автоматического решения основных проблем многокритериальной вероятностно-временной оценки защищенности сложных информационно-технических интерфейсов (т.е., в нашем случае, возможностью нормализации компонент векторных МЗ ИРПЗ и их свертки) в рамках выбранного вероятностного подхода к анализу информационной безопасности объектов такого класса.

Основа данного метода заключается в пошаговом (поэтапном) расчете ЧСМЗ на любом конкретном шаге оценивания и их математически корректной «свертке» в ВКМЗ ИРПЗ на цифровых ресурсах ЦОД на этом же шаге. С точки зрения математической корректности, этот метод может быть осуществлен на основе аппарата условных вероятностей, а также классических теорем функциональной и параметрической декомпозиции. При этом вероятностная комплексная МЗ ИРПЗ формируется из условных вероятностей выполнения критериев (требований) по отдельным частным субметрикам защищенности ИРПЗ на цифровых ресурсах ЦОД — условных вероятностей выполнения критериев (требований) по доступности, конфиденциальности и целостности.

Причем, формулировку отдельной вероятностной ЧСМЗ интерфейсов такого класса, характеризующей, например, аспект защищенности ИРПЗ, традиционно ориентированный на безопасную доступность данных, можно осуществить на основе (в виде) условной вероятности выполнения требований к:

- вероятности своевременного защищенного доступа к цифровым ресурсам ЦОД с использованием ИРПЗ;
- среднему времени защищенного доступа к цифровым ресурсам ЦОД с использованием ИРПЗ;
- и среднему времени до отказа в доступе к цифровым ресурсам ЦОД с использованием ИРПЗ [6].

Таким образом, рассмотрены этапы решения задачи обоснования и корректной математической формулировки вероятностной комплексной метрики и отдельных частных субметрик защищенности пользовательских интерфейсов для реализации поисковых запросов на ресурсах центров обработки данных.

Разработанная вероятностная комплексная метрика призвана гарантировать точный текущий и прогнозный контроль уровня защищенности пользовательских интерфейсов для реализации поисковых запросов, она создана на базе обобщенной условной вероятности выполнения критериев выполнения требований по отдельным частным субметрикам защищенности, характеризующим доступность, конфиденциальность и целостность ИРПЗ.

Исследованные подходы к формулировке частных субметрик защищенности интерфейсов могут лечь в основу перспективных направлений для создания на их базе алгоритмов точного и своевременного контроля информационной безопасности объектов такого класса. При этом предложенный подход отличается гибкостью и многофункциональностью, а конгломерат метода вероятностной скаляризации и математического аппарата условных вероятностей предопределяет возможность достоверного и оперативного прогностического анализа защищенности подобных интерфейсов для реализации поисковых запросов.



## СПИСОК ЛИТЕРАТУРЫ

1. Исхаков А.Ю., Жарко Е.Ф. Подход к защите интерфейсов управления киберфизической системой от угроз нарушения доступности // Информационные и математические технологии в науке и управлении. 2023. №1(29). С. 149-157.
2. Паращук И.Б., Чечулин А.А. Сущность и содержание задач поиска уязвимостей интерфейсов в интересах безопасного управления беспилотными транспортными средствами «умного города» // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2020). IX Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. / Под. ред. С.В. Бачевского; сост. А. Г. Владыко, Е.А. Аникевич. СПб.: СПбГУТ, 2020. Т.1. С. 759-763.
3. Национальный стандарт РФ ГОСТ Р 52633.4-2011. Защита информации. Техника защиты информации. Интерфейсы взаимодействия с нейросетевыми преобразователями биометрии код доступа. М.: СтандартИнформ. 2012. 102 с.
4. Утехин И.В. Поиск и его интерфейсы // Laboratorium: журнал социальных исследований. 2019. №11(1). С. 152-165.
5. Саяркин В.А., Виноградов В.Р., Паращук И.Б. Контроль эффективности и надежности системы комплексной безопасности для обеспечения защищенности доверенных иммерсивных интерфейсов взаимодействия робота и оператора // Экстремальная робототехника. 2024. № 1(35). С. 27-31.
6. Саяркин В.А., Крюкова Е.С., Паращук И.Б. Средняя за интервал времени оценка защищенности и анализ рисков информационной безопасности интерфейсов взаимодействия робота и оператора // Экстремальная робототехника. Труды 34-й Международной научно-технической конференции «Экстремальная робототехника», 23-24 ноября 2023 г. СПб.: Изд-во ЦНИИ РТК, 2023. С. 19-26.

УДК 004.94

**ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТИ  
БЕСПРОВОДНОЙ ПЕРЕДАЧИ ДАННЫХ LORA****Сильчев Кирилл Владимирович**

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)  
Профессора Попова ул., 5, Санкт-Петербург, 197022, Россия  
e-mail: silchev\_kirill@mail.ru

**Аннотация.** Рассмотрена организация безопасной беспроводной передачи данных с применением беспроводной технологии LoRa сети LoRaWAN. Оценены возможности разработанного и апробированного программного метода гарантированной безопасной беспроводной передачи данных, методики исследования эффективности методов модификации аппаратно-программного комплекса организации передачи данных, методологии процесса тестирования передатчика данных LoRa. Рассматривается подход с сочетанием аппаратного и программного решения для обеспечения передачи пакетов данных между устройствами беспроводной сети.

**Ключевые слова:** безопасные информационные системы; моделирование беспроводной передачи данных; беспроводная технология LoRa; работа сетевых устройств беспроводной сети передачи данных.

**ENSURING THE INFORMATION SECURITY OF THE LORA WIRELESS  
DATA TRANSMISSION NETWORK****Silchev Kirill**

St. Petersburg State Electrotechnical University «LETI»  
5 Professor Popov St, St. Petersburg, 197022, Russia  
e-mail: silchev\_kirill@mail.ru

**Abstract.** The article discusses the organization of secure wireless data transmission using the LoRaWAN wireless technology. It evaluates the capabilities of the developed and tested software method for guaranteed secure wireless data transmission, the methods for studying the effectiveness of modifying the hardware and software complex for data transmission, and the methodology for testing the LoRa data transmitter. This approach combines hardware and software solutions to transmit data packets between wireless network devices.

**Keywords:** secure information systems; wireless data transmission modeling; LoRa wireless technology; operation of wireless data transmission network devices.

Основным методом применения беспроводной технологии LoRa являются сети LoRaWAN. Сеть использует топологию «звезда» и каждое устройство взаимодействует с базовой станцией напрямую. Для сетей городского или регионального масштаба применяется конфигурации «звезда из звезд», когда устройство или модем с LoRa-модулем передают данные по радиоканалу на базовую станцию. Станция в радиусе своего действия принимает сигналы от всех устройств, оцифровывает и передает на удаленный сервер, где данные используются для отображения, анализа, подготовки отчетов и принятия решений. Управление устройствами сети происходит с использованием обратного канала связи. Обеспечивающими каналами связи могут быть Ethernet, VSAT, сотовая связь. Рассматривается подход с сочетанием аппаратного и программного решения для обеспечения передачи пакетов данных между устройствами беспроводной сети [1, 2].

Предпочтением сети LoRaWAN и технологии LoRa является возможность передачи данных на большие расстояния с минимальным энергопотреблением через модули радиосвязи, работающие на частотах от нескольких десятков до нескольких сотен мегагерц, что позволяет обеспечить дальность передачи данных до нескольких километров при минимальной мощности сигнала. Наиболее эффективна такая сеть в условиях с передачей данных на расстояния с минимальным энергопотреблением и низкими затратами на поддержку сети, например, для потребителей регионального сельского хозяйства, промышленности, здравоохранения. Возможно

использование в проектах умного города за счет функционального определения местоположения устройств методом трилатерации через временные метки от интернет-шлюзов [3].

Для обеспечения гарантированной передачи небольшого объема данных и возможности длительной работы сетевых устройств от автономных источников питания на увеличенной территории охвата беспроводной сетью, возможно применение приложений с использованием двух модулей LoRa по принципу Peer-to-Peer (P2P) и метода Radio Head Packet Method. На программном уровне [4–6] использовалась библиотека LoRa от SandeepMistry, функция передачи данных запускается строкой `LoRa.begin` так, что устройство готово передавать пакет между `LoRa.beginPacket()` и `LoRa.endPacket()`. Пакет может быть в любом формате переменных, но для обеспечения простоты подсчета и оптимизации будет использоваться массив `char`. Скорость передачи данных может достигать от 0,3 кбит/сек до 50 кбит/сек в зависимости от коэффициента расширения. Минусом широкого использования предлагаемого подхода является сложность обеспечения корректной работы устройств, если в радиусе примерно 5 км работы присутствует другое активное передающее устройство LoRa [7].

На физическом уровне принципа передачи данных технологии LoRa PHY лежит свойство радиосистем усиления энергии (а значит и увеличения дальности связи) при уменьшении скорости передачи. Чем ниже битовая скорость передачи, тем больше энергии вкладывается в каждый бит и тем легче выделить его на фоне шумов в приемной части системы. Таким образом, низкая скорость передачи данных позволяет добиться большей дальности их приема и поддержания необходимого уровня безопасного доведения данных.

Апробация подхода показала, что за счет сжатия пакетов передачи данных для сокращения длительности окна связи уменьшается длительность передачи данных и заметно повышается вероятность доставки информации. Для передачи данных можно использовать ограниченное окно, в котором устройство находится в эфире, и шифрование данных перед отправкой. При этом дополнительно будут снижены аппаратные и временные затраты на передачу пакета данных.

Для противодействия интерференциям возможно использовать сканирование канала. Данный программный метод позволяет обрабатывать данные из радиозфира, чтобы корректно выбирать рабочие частоты для передачи данных, для этого к функционалу стандарта LoRaWAN возможно подключение дополнительного модуля.

Таким образом, предложенный подход обеспечения информационной безопасности сети беспроводной передачи данных LoRa с разработанным и апробированным программным методом обеспечивает обработку данных из радиозфира позволяет:

- сократить энергозатраты устройства;
- уменьшить нагрузку на эфир, тем самым снизив наведение на работы прочих устройств LoRa;
- разработать методику исследования эффективности методов модификации аппаратно-программного комплекса;
- вывести основные предложения по модификации устройства;
- подготовить основу методологии процесса тестирования передатчика данных LoRa.

Ограничением применения действующего варианта предложенного подхода обеспечения гарантированной безопасной беспроводной передачи данных является отмеченное заключение, что с увеличением расстояния от передатчика до приемника, длительность окна передачи варьируется и оба устройства не могут точно согласовать время связи и возможна рассинхронизация окон. В этом случае при дальнейшем увеличении расстояния передача данных может быть нарушена.

## СПИСОК ЛИТЕРАТУРЫ

1. What is LoRa? // Semtech Official Website. <https://www.semtech.com/lora/what-is-lora> (дата обращения 21.09.2024).
2. Adelantado Ferran, Vilajosana Xavier, Tuset-Peiro Pere, Martinez Borja, Melia-Segui Joan, Watteyne Thomas. Understanding the Limits of 3. LoRaWAN // IEEE Communications Magazine, 2017, pp. 34–40.
3. Marco Centenaro, Lorenzo Vangelista, Andrea Zanella, Michele Zorzi. Long-Range Communications in Unlicensed Bands: the Rising Stars in the IoT and Smart City Scenarios // IEEE Wireless Communications, октябрь 2016, pp. 22–28.
4. SX1278 Specification // Github. <https://github.com/IOT-MCU> (дата обращения 30.11.2024).
5. The NMEA 0183 Protocol. <http://www.tronico.fi/ON6NT/docs/NMEA0183.pdf> (дата обращения 15.06.2024).
6. Контент u-blox 6 GPS Modules Data Sheet. [https://content.u-blox.com/sites/default/files/products/documents/NEO-6\\_DataSheet\\_%28GPS.G6-HW-09005%29.pdf](https://content.u-blox.com/sites/default/files/products/documents/NEO-6_DataSheet_%28GPS.G6-HW-09005%29.pdf) (дата обращения 15.06.2024).
7. B2Field. Что такое LBS. <https://b2field.com/ru/blog/chto-takoe-lbs/> (дата обращения 10.06.2024).

УДК 004.8

## ГЛУБОКОЕ ОБУЧЕНИЕ ДЛЯ ОБНАРУЖЕНИЯ АНОМАЛИЙ В СЕТЕВОМ ТРАФИКЕ

Ситдиков Дмитрий Сергеевич<sup>1</sup>, Лешинский Богдан Сергеевич<sup>1</sup>, Шевченко Александр Александрович<sup>2</sup>

<sup>1</sup> Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

<sup>2</sup> Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Большевицкое пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

e-mails: dima.sitdikov.99@mail.ru, leshinski\_bog@bk.ru, alex\_pavel1991@mail.ru

**Аннотация.** Рост сложности атак и объемов трафика в современных сетях делает традиционные сигнатурные и пороговые методы недостаточно гибкими и точными. В работе представлен обзор применения глубокого обучения (DL) для обнаружения аномалий и вторжений в сетевом трафике операторского уровня.

Показано, что нейросетевые модели способны автоматически извлекать пространственно-временные закономерности, учитывать сезонность и динамику нагрузки, что уменьшает долю ложных срабатываний и повышает полноту обнаружения. Отмечены практики работы с дисбалансом классов и редкими атаками, включая перенос обучения и специализированные процедуры обучения. Обсуждаются вопросы производительности и внедрения в реальном времени, а также необходимость объяснения решений при эксплуатации. Результаты недавних исследований демонстрируют эффективность трансформерных архитектур и гибридных конвейеров для промышленных сценариев.

**Ключевые слова:** глубокое обучение; IDS; CNN; RNN; Transformer; обнаружение аномалий.

## DEEP LEARNING FOR ANOMALIES DETECTION IN NETWORK TRAFFIC

Sitdikov Dmitry<sup>1</sup>, Leshchinsky Bogdan<sup>1</sup>, Shevchenko Alexander<sup>2</sup>

<sup>1</sup> The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny  
3 Tikhoretsky Av, St. Petersburg, 194064, Russia

<sup>2</sup> The Bonch-Bruевич Saint Petersburg State University of Telecommunications  
22 Bolshhevikov Av, bldg 1, St. Petersburg, 193232, Russia

e-mails: dima.sitdikov.99@mail.ru, leshinski\_bog@bk.ru, alex\_pavel1991@mail.ru

**Abstract.** The increasing complexity of attacks and traffic volumes in modern networks make traditional signature- and threshold-based methods inflexible and inaccurate enough. This paper presents an overview of deep learning (DL) applications for anomaly and intrusion detection in carrier-grade network traffic. It is shown that neural network models are able to automatically extract spatio-temporal patterns, take into account seasonality and load dynamics, which reduces the proportion of false positives and increases detection completeness. Practices for dealing with class imbalance and rare attacks, including transfer learning and specialized learning procedures, are noted. Performance and real-time implementation issues are discussed, as well as the need to explain operational decisions. Recent research results demonstrate the effectiveness of transformer architectures and hybrid pipelines for industrial scenarios.

**Keywords:** deep learning; NIDS; CNN; RNN; Transformer; anomaly detection.

Интеграция моделей глубокого обучения в сетевые системы обнаружения вторжений снижает зависимость от ручной инженерии признаков и позволяет выявлять сложные зависимости в пакетах и потоках данных. В условиях высокоскоростных многодоменных сетей (операторские магистрали, дата-центры, сегменты Интернета вещей) аномалиями считаются отклонения интенсивности, структуры и контекста взаимодействий. Классические правила и сигнатуры плохо масштабируются к динамичным профилям нагрузки и новым атакам; модели глубокого обучения, обученные на исторических данных, улавливают устойчивые закономерности, отличающие «норму» от инцидента [1, 2].

Свёрточные нейронные сети хорошо работают с «пространственными» представлениями потоков и помогают распознавать характерные комбинации признаков для атак отказа в обслуживании, сканирования или утечки данных [1-3]. Рекуррентные архитектуры (в том числе LSTM) учитывают последовательную природу взаимодействий и интервалы между пакетами, фиксируя сдвиги суточной/недельной сезонности и «цепочки» шагов составных атак [2, 3].

Модели трансформеры, обучаемые на представлениях потоков, демонстрируют высокую способность к обобщению ранее не наблюдавшихся шаблонов и повышают качество по редким классам за счёт механизма внимания и более длинного «эффективного контекста» [4, 5]. В опубликованных работах по потоковой детекции показано, что корректная предобработка (нормализация, агрегация), а также балансировка/взвешивание классов заметно повышают устойчивость и стабильность показателей качества [4, 5]. Особое значение для промышленной эксплуатации имеет работа в режиме реального времени. Для снижения задержек применяют квантование и прореживание весов, что позволяет исполнять модели на периферийных узлах сети (узлах телеметрии, платформах периферийных вычислений) с минимальным снижением точности, важной для операторов связи [1, 6]. При этом гибридные схемы, когда быстрые «лёгкие» модели выполняют первичную фильтрацию потока и передают подозрительные подпотоки более сложным классификаторам, помогают поддерживать целевые показатели уровня сервиса и не перегружать вычислительные ресурсы [4, 6].

Важной проблемой остается дисбаланс классов и доменная изменчивость трафика между сегментами. Эффективными показали себя перенос обучения и специальные функции потерь, повышающие полноту по малочисленным классам без заметного роста ложных срабатываний [2, 5]. Для работы центров мониторинга и реагирования на инциденты важна объяснимость: даже при использовании сложных архитектур в конвейер добавляют механизмы интерпретации решений, подсказывающие аналитикам, какие показатели привели к срабатыванию и как изменился бы исход при иных значениях признаков [1, 2]. Ряд исследований отмечает, что такие объяснения ускоряют разбор инцидентов [1, 2, 6]. Наконец, для промышленных сценариев полезны потоковые метрики качества (AUC-PR, F1 для редких классов, задержка обнаружения), они лучше отражают требования к мониторингу, чем усреднённые оценки по отложенным наборам данных [1, 4].

Глубокое обучение стало ключевой технологией для обнаружения аномалий в сетевом трафике: за счёт автоматического извлечения пространственно-временных признаков, учёта сезонности и более точной работы с

редкими классами модели повышают полноту и снижают долю ложных срабатываний по сравнению с классическими подходами [1-3].

Трансформеры и гибридные конвейеры подтверждают применимость в реальном времени при должной оптимизации и корректной организации потоковой предобработки [4-6]. Для успешной эксплуатации критичны объяснимость решений и инженерия производительности (периферийное исполнение, квантование, прореживание весов). Сочетание этих практик превращает детекцию аномалий в проактивный инструмент обеспечения устойчивости и безопасности телекоммуникационных сетей.

#### СПИСОК ЛИТЕРАТУРЫ

1. Chinnasamy R. et al. Deep learning-driven methods for network-based intrusion detection systems: A systematic review //ICT Express. 2025.
2. Song Y. et al. Application of deep learning in malware detection: a review //Journal of Big Data. 2025. Т. 12. №. 1. С. 99.
3. Lampe B., Meng W. A survey of deep learning-based intrusion detection in automotive applications //Expert Systems with Applications. 2023. Т. 221. С. 119771.
4. Manocchio L. D. et al. Flowtransformer: A transformer framework for flow-based network intrusion detection systems //Expert Systems with Applications. 2024. Т. 241. С. 122564.
5. Ullah F. et al. IDS-INT: Intrusion detection system using transformer-based transfer learning for imbalanced network traffic //Digital Communications and Networks. 2024. Т. 10. №. 1. С. 190-204.
6. Li Z. et al. Toward Deep Learning based Intrusion Detection System: A Survey //Proceedings of the 2024 6th International Conference on Big Data Engineering. 2024. С. 25-32.

УДК 004.8

### ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОММУНИКАЦИЙ ИНТЕРНЕТА ВЕЩЕЙ

Ситдиков Дмитрий Сергеевич<sup>1</sup>, Лешинский Богдан Сергеевич<sup>1</sup>, Шевченко Александр Александрович<sup>2</sup>

<sup>1</sup> Военная академия связи им. Маршала Советского Союза С. М. Буденного  
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

<sup>2</sup> Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mails: dima.sitdikov.99@mail.ru, leshinski\_bog@bk.ru, alex\_pavel1991@mail.ru

**Аннотация.** Экосистема IoT объединяет миллиарды разнородных узлов, при этом устройства ограничены по энергии/памяти, а протоколы и трафик крайне неоднородны, что увеличивает поверхность атаки. В работе обобщены подходы на основе искусственного интеллекта к защите коммуникаций IoT: поведенческое профилирование и обнаружение аномалий, лёгкие модели и edge AI для анализа «на краю», а также federated learning, повышающие масштабируемость и приватность. Отмечены приёмы снижения ложных срабатываний, использование автоэнкодеров для безнадзорного выявления отклонений, а также практики генерации синтетических аномалий (GAN) и адаптивной настройки порогов/реакций методами обучения с подкреплением. Показано, что интеграция перечисленных техник повышает полноту обнаружения и устойчивость IoT-инфраструктур к современным угрозам.

**Ключевые слова:** IoT; безопасность; машинное обучение; аномалии; edge AI; автоэнкодер.

### ARTIFICIAL INTELLIGENCE FOR SECURING INTERNET OF THINGS COMMUNICATIONS

Sitdikov Dmitry<sup>1</sup>, Leshchinsky Bogdan<sup>1</sup>, Shevchenko Alexander<sup>2</sup>

<sup>1</sup> The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny  
3 Tikhoretsky Av, St. Petersburg, 194064, Russia

<sup>2</sup> The Bonch-Bruевич Saint Petersburg State University of Telecommunications  
22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia

e-mails: dima.sitdikov.99@mail.ru, leshinski\_bog@bk.ru, alex\_pavel1991@mail.ru

**Abstract.** The IoT ecosystem unites billions of heterogeneous nodes, while the devices are limited in energy/memory, and the protocols and traffic are extremely heterogeneous, which increases the attack surface. The paper summarizes artificial intelligence-based approaches to protecting IoT communications: behavioral profiling and anomaly detection, lightweight models and edge AI for analysis «at the edge», as well as federated learning, which improve scalability and privacy. The paper highlights techniques for reducing false positives, using autoencoders for unsupervised detection of deviations, as well as practices of generating synthetic anomalies (GAN) and adaptive threshold/response adjustment using reinforcement learning methods. It is shown that the integration of these techniques increases the completeness of detection and the resilience of IoT infrastructures to modern threats.

**Keywords:** IoT security; anomaly detection; edge AI; lightweight ML; autoencoder.

Ограниченные вычислительные ресурсы и малая энергоэффективность узлов Интернета Вещей (IoT) принципиально смещают комплексный анализ сетевого трафика от периферийных устройств к более мощным шлюзам и на край сети (edge computing). Это позволяет распределить нагрузку, оставив на конечных устройствах лишь базовую предобработку данных. Развитие технологий edge AI (искусственного интеллекта на грани сети) позволяет не только выявлять вторжения в режиме, приближенном к реальному времени, но и делает это, не перегружая каналы связи и централизованные системы мониторинга облачного уровня.

Ключевой принцип заключается в том, что наверх передаются не сырые данные, а лишь агрегированные «сводки» и метаданные, касающиеся только выявленных аномалий и угроз, что радикально экономит пропускную способность [1, 2].

В основе таких систем лежат поведенческие профили устройств, созданные на основе машинного обучения (ML), которые учатся отличать легитимную фоновую активность устройств от подозрительных командно-контрольных (C&C) паттернов, характерных для ботнетов.

Для анализа последовательностей сетевых пакетов особенно эффективны методы глубокого обучения (DL), такие как рекуррентные нейронные сети (RNN) и их специализированные версии с долгой краткосрочной памятью (LSTM), которые способны улавливать сложные временные зависимости в потоках данных. Одномерные сверточные нейронные сети (1D-CNN) успешно извлекают скрытые локальные признаки и паттерны в заголовках пакетов. Для обнаружения ранее неизвестных атак бесценны автоэнкодеры, работающие по принципу обучения без учителя: они обучаются на нормальном трафике и затем обнаруживают любые, даже малые, отклонения от эталона, не требуя заранее составленных сигнатур [3].

Для практической эксплуатации в реальных сетях критически важно снижать долю ложных срабатываний (False Positive Rate), которые подрывают доверие к системе и перегружают операторов. Для стабилизации метрик качества и повышения надежности детекции широко применяются ансамбли моделей (ensemble methods), которые агрегируют предсказания нескольких классификаторов, компенсируя их индивидуальные ошибки [4].

Масштаб развертывания IoT и вопросы приватности данных успешно решаются с помощью федеративного обучения (federated learning): эта парадигма позволяет узлам или шлюзам тренировать локальные модели на своих данных, а затем делиться только обновлениями параметров (весов) с глобальной моделью, которая агрегирует эти знания. Это не только сохраняет данные на месте, но и особенно полезно в условиях неоднородности (non-IID) данных различных устройств и сред [5].

Для искусственного расширения обучающей выборки, особенно для редких типов атак, и повышения устойчивости моделей к новым, неизвестным сценариям применяют генеративно-состязательные сети (GAN). Они генерируют синтетические данные атак, чтобы сбалансировать датасеты и улучшить обучение моделей.

Обучение с подкреплением (RL) помогает адаптивно и динамически настраивать пороги классификации на основе обратной связи от среды и автоматизировать процессы ответа на инциденты, минимизируя вмешательство человека. Типичные успешные примеры внедрения включают выявление ботнетов семейства Mirai, атак DDoS в экосистемах «умного дома» и промышленном IoT; при этом использование легких (lightweight) моделей и техник компрессии, позволяют выполнять детекцию прямо на граничных узлах с ограниченными ресурсами.

Для успешной эксплуатации в продакшн-средах крайне важны не только сами алгоритмы, но и генерация интерпретируемых отчетов для аналитиков безопасности, отслеживание потоковых метрик качества, таких как AUC-PR (кривая точности-полноты), которая информативнее AUC-ROC при сильном дисбалансе классов.

Таким образом, комбинация ML/DL-детекторов, архитектуры edge AI и парадигмы federated learning формирует целостную, масштабируемую и учитывающую приватность данных стратегию защиты IoT-коммуникаций: в результате повышается полнота (recall) и своевременность обнаружения, системно снижается доля ложных срабатываний, а реакция на инциденты становится проактивной и адаптивной к новым эволюционирующим атакам и сбоям в сети.

#### СПИСОК ЛИТЕРАТУРЫ

1. Alfahaid A. et al. Machine Learning-Based Security Solutions for IoT Networks: A Comprehensive Survey //Sensors. 2025. Т. 25. №. 11. С. 3341.
2. Haider Z. A. et al. A Survey on anomaly detection in IoT: Techniques, challenges, and opportunities with the integration of 6G //Computer Networks. 2025. С. 111484.
3. DeMedeiros K., Hendawi A., Alvarez M. A survey of AI-based anomaly detection in IoT and sensor networks //Sensors. 2023. Т. 23. №. 3. С. 1352.
4. Dubey K. et al. A review of IoT security: machine learning and deep learning perspective //Procedia Computer Science. 2024. Т. 235. С. 335-346.
5. Rhachi H., Balboul Y., Bouayad A. Enhanced Anomaly Detection in IoT Networks Using Deep Autoencoders with Feature Selection Techniques // Sensors. 2025. Т. 25. №. 10. С. 3150.

УДК 004.8

#### ОБЪЯСНИМЫЙ ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В СИСТЕМАХ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Ситдиков Дмитрий Сергеевич<sup>1</sup>, Лещинский Богдан Сергеевич<sup>1</sup>, Шевченко Александр Александрович<sup>2</sup>

<sup>1</sup> Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

<sup>2</sup> Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

e-mails: dima.sitdikov.99@mail.ru, leshinski\_bog@bk.ru, alex\_pavel1991@mail.ru

**Аннотация.** Внедрение методов искусственного интеллекта в сети связи повышает эффективность обнаружения кибератак, но сопровождается проблемой «чёрного ящика»: решения сложных моделей остаются непонятными для человека. Объяснимый ИИ (XAI) призван сделать работу алгоритмов прозрачной и повысить доверие к ним. В работе рассматривается роль XAI в системе обнаружения вторжений (IDS) телекоммуникационных сетей. Актуальность темы обусловлена необходимостью понимания причин, по

которым модель помечает сетевой трафик как вредоносный или безопасный. Показано, что использование XAI позволяет специалистам по безопасности интерпретировать решения моделей, корректно настраивать политики и быстрее локализовать первопричины инцидентов, что повышает эффективность реагирования и доверие к ИИ-системам при эксплуатации в реальном времени.

**Ключевые слова:** объяснимый ИИ; XAI; IDS; SHAP; LIME; интерпретируемость.

## EXPLAINABLE ARTIFICIAL INTELLIGENCE IN TELECOMMUNICATION NETWORK INTRUSION DETECTION SYSTEMS

Sitdikov Dmitry<sup>1</sup>, Leshchinsky Bogdan<sup>1</sup>, Shevchenko Alexander<sup>2</sup>

<sup>1</sup> The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny  
3 Tikhoretsky Av, St. Petersburg, 194064, Russia

<sup>2</sup> The Bonch-Bruевич Saint Petersburg State University of Telecommunications  
22 Bolshevnikov Av, bldg 1, St. Petersburg, 193232, Russia

e-mails: dima.sitdikov.99@mail.ru, leshinski\_bog@bk.ru, alex\_pavel1991@mail.ru

**Abstract.** The introduction of artificial intelligence methods in communication networks increases the efficiency of detecting cyberattacks, but is accompanied by the problem of the «black box»: the solutions of complex models remain incomprehensible to humans. Explainable AI (XAI) is designed to make the work of algorithms transparent and increase trust in them. The paper considers the role of XAI in the intrusion detection system (IDS) of telecommunication networks. The relevance of the topic is due to the need to understand the reasons why the model marks network traffic as malicious or safe. It is shown that the use of XAI allows security specialists to interpret model decisions, correctly configure policies and quickly localize the root causes of incidents, which increases the effectiveness of response and trust in AI systems when operating in real time.

**Keywords:** explainable AI; IDS; SHAP; LIME; interpretability.

Интеллектуальные системы обнаружения вторжений, основанные на передовых методах машинного (ML) и глубокого обучения (DL), демонстрируют исключительно высокую точность в классификации сложных и замаскированных кибератак, превосходя по этому показателю традиционные сигнатурные методы. Однако фундаментальная проблема таких систем заключается в их непрозрачности («black box»): аналитик безопасности зачастую не может понять логику, по которой модель приняла то или иное решение, что критически затрудняет проведение аудитов, расследование инцидентов и оперативное реагирование. Для решения этой проблемы активно развивается подход Объяснимого ИИ, который дополняет сложные модели, обеспечивая как локальные объяснения для конкретного предсказания (например, для отдельной подозрительной сессии), так и глобальные, описывающие общее поведение модели на всем датасете. Такие техники, как LIME (Local Interpretable Model-agnostic Explanations) и SHAP (SHapley Additive exPlanations), позволяют количественно оценить и визуализировать вклад каждого признака, например IP-адрес, порт, размер пакета в итоговое решение модели для конкретного случая, значительно повышая доверие к системе и её управляемость со стороны человека-оператора [1].

Современные исследования и практические внедрения показывают, что XAI-техники можно эффективно и органично внедрять в рабочий конвейер IDS, не вызывая существенного роста вычислительной задержки, что позволяет сохранить высокое качество классификации в режиме, близком к реальному времени, и одновременно кардинально облегчить процессы отладки и валидации моделей [2]. При этом ученые подчеркивают острую необходимость адаптации общих методов XAI к специфическим особенностям сетевого трафика: ключевыми проблемами остаются влияние сильного дисбаланса классов (нормальный трафик на порядки превышает атаки) и работы с высокоразмерными признаками на стабильность, точность и достоверность генерируемых объяснений, что требует разработки специализированных методов [3, 4].

Наряду с развитием методов объяснения уже готовых моделей «чёрных ящиков» (post-hoc объяснения), в научном сообществе растёт закономерный интерес к изначально интерпретируемым архитектурам (например, основанным на деревьях решений с налагаемыми ограничениями) и гибридным ансамблевым подходам. В таких системах внешние post-hoc объяснения эффективно дополняются встроенной, внутренней интерпретируемостью (intrinsic interpretability) некоторых компонентов системы, что в совокупности создает более целостную и надежную картину принятия решений [5, 6].

В контексте высокоскоростных и слабоструктурированных связей в сетях 5G и IoT развертывание XAI становится не просто опцией, а необходимостью: он помогает сетевым операторам быстро локализовать первопричины срабатываний, документировать факторы риска для отчетности, что крайне важно, итеративно снижать число ложных тревог, тонко настраивая пороги срабатывания на основе полученных объяснений. Таким образом, Объяснимый ИИ является одним из наиболее перспективных и стратегически важных направлений в современной кибербезопасности сетей связи. Его практическое использование дает уникальную возможность трансформировать «чёрный ящик» сложных моделей в прозрачную и аудируемую систему, что ведет к закономерному росту доверия со стороны специалистов по безопасности, менеджмента и надзорных органов. В итоге, комплексная интеграция XAI в системы обнаружения вторжений способствует не только более быстрому, но и гораздо более обоснованному, аргументированному принятию решений, что в конечном счете повышает безопасность телекоммуникационных инфраструктур.

## СПИСОК ЛИТЕРАТУРЫ

1. Arreche O., Guntur T., Abdallah M. Xai-ids: Toward proposing an explainable artificial intelligence framework for enhancing network intrusion detection systems //Applied Sciences. 2024. T. 14. №. 10. C. 4170.
2. Hermosilla P., Berrios S., Allende-Cid H. Explainable AI for Forensic Analysis: A Comparative Study of SHAP and LIME in Intrusion Detection Models //Applied Sciences. 2025. T. 15. №. 13. C. 7329.
3. Mohale V. Z., Obagbuwa I. C. A systematic review on the integration of explainable artificial intelligence in intrusion detection systems to enhancing transparency and interpretability in cybersecurity //Frontiers in Artificial Intelligence. 2025. T. 8. C. 1526221.
4. Samed A. L., Sagioglu S. Explainable artificial intelligence models in intrusion detection systems //Engineering Applications of Artificial Intelligence. 2025. T. 144. C. 110145.
5. Ahmed U. et al. Explainable AI-based innovative hybrid ensemble model for intrusion detection //Journal of Cloud Computing. 2024. T. 13. №. 1. C. 150.
6. Corea P. M. et al. Explainable ai for comparative analysis of intrusion detection models //2024 IEEE International Mediterranean Conference on Communications and Networking (MeditCom). IEEE, 2024. C. 585-590.

УДК 004.056.5:004.032.26

**ПРАКТИКИ ДОВЕРИЯ К ML-МОДЕЛЯМ: КОНТРОЛЬ SHA-256 И СРАВНЕНИЕ ПОВЕДЕНИЯ  
PYTORCH И TENSORFLOW ПОСЛЕ ДЕСЕРИАЛИЗАЦИИ**

**Ситдиков Дмитрий Сергеевич<sup>1</sup>, Лещинский Богдан Сергеевич<sup>1</sup>, Шевченко Александр Александрович<sup>2</sup>**

<sup>1</sup> Военная академия связи им. Маршала Советского Союза С. М. Буденного  
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

<sup>2</sup> Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевики пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mails: dima.sitdikov.99@mail.ru, leshinski\_bog@bk.ru, alex\_pavel1991@mail.ru

**Аннотация.** Усиление требований к безопасности цепочки поставок ПО затрагивает и машинное обучение: модели передаются между командами и средами, что требует проверки их подлинности и целостности. В работе рассматриваются практики доверия к ML-моделям: криптографическая подпись артефактов (инициатива OpenSSF Model Signing) и контроль целостности с помощью SHA-256; особенности сериализации и загрузки в TensorFlow/Keras (формат SavedModel, «сигнатуры», параметр безопасной загрузки `safe_mode`) и их ограничения, а также подход PyTorch к сохранению `state_dict` и режим загрузки `weights_only`. Проведён прикладной эксперимент на идентичной MLP-архитектуре в PyTorch и TensorFlow: обученные модели сохраняются, для файлов вычисляются SHA-256 до/после загрузки и сравниваются предсказания исходных и загруженных экземпляров. Получено совпадение хеш-сумм и функциональной эквивалентности, что подтверждает корректность механизмов сериализации при надлежащем использовании. Обсуждаются риски десериализации (обход `safe_mode`, угрозы pickle) и формулируются рекомендации: подписывать модели и проверять подписи на каждом этапе CI/CD, хранить и переносить преимущественно веса (`state_dict`), включать `safe_mode` в Keras и `weights_only` в PyTorch, а также вести аудит загрузок.

**Ключевые слова:** доверие к моделям; целостность; SHA-256; цифровая подпись; десериализация; TensorFlow/Keras; PyTorch.

**TRUST PRACTICES FOR ML MODELS: SHA-256 INTEGRITY CONTROL AND BEHAVIORAL  
PARITY OF PYTORCH AND TENSORFLOW AFTER DESERIALIZATION**

**Sitdikov Dmitry<sup>1</sup>, Leshchinsky Bogdan<sup>1</sup>, Shevchenko Alexander<sup>2</sup>**

<sup>1</sup> The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny  
3 Tikhoretsky Av, St. Petersburg, 194064, Russia

<sup>2</sup> The Bonch-Bruевич Saint Petersburg State University of Telecommunications  
22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia

e-mails: dima.sitdikov.99@mail.ru, leshinski\_bog@bk.ru, alex\_pavel1991@mail.ru

**Abstract.** Software supply-chain security extends to ML: models circulate across teams and environments, so authenticity and integrity must be verified. We review model signing (OpenSSF) and SHA-256 integrity checks, TensorFlow/Keras serialization (SavedModel, signatures, `safe_mode`) and its limitations, and PyTorch's `state_dict` with the `weights_only` loading mode. An experiment with an identical MLP in PyTorch and TensorFlow computes SHA-256 before/after loading and compares predictions; hashes match and outputs remain equivalent, indicating correct serialization when used properly. We discuss deserialization risks (`safe_mode` bypass, pickle threats) and recommend signing models, verifying signatures throughout CI/CD, transporting weights, enabling Keras `safe_mode` and PyTorch `weights_only`, and auditing loads.

**Keywords:** model trust; integrity; SHA-256; digital signing; deserialization; TensorFlow/Keras; PyTorch.

Современные практики CI/CD в ML требуют не только высокой воспроизводимости, но и проверяемого доверия к артефактам. Подход OpenSSF Model Signing рекомендует подписывать модели с использованием открытых ключей и проверять подпись при каждом переносе артефакта (репозиторий, деплой, повторное использование) [1]. Контроль целостности дополняется вычислением SHA-256; устойчивость к коллизиям и лавинообразный эффект делают хеш-проверку эффективной для выявления любых изменений файла [2]. В экосистеме TensorFlow стандартный SavedModel сохраняет структуру, веса и «сигнатуры» вызовов, а параметр

safe\_mode (Keras) снижает риск выполнения произвольного кода при загрузке, однако показаны векторы обхода, поэтому требуются дополнительные меры [3, 4]. В PyTorch рекомендуется сохранять именно state\_dict и при загрузке использовать weights\_only=True, минимизируя поверхность атаки механизма pickle [5].

Этапы проведения экспериментов:

1. Подготовка данных (масштабирование, стратификация).
2. Построение одинаковой MLP в PyTorch и TensorFlow.
3. Обучение — 30 эпох, batch 32, оптимизатор Adam.
4. Сохранение: state\_dict в .pth и модель в формате .keras.
5. Вычисление SHA-256 файлов.
6. Загрузка моделей и повторная проверка хешей.
7. Сравнение предсказаний исходных и загруженных моделей на одинаковых примерах.

Результаты и обсуждение. Хеш-суммы совпали для обеих реализаций, а предсказания после загрузки соответствуют исходным (функциональная эквивалентность). Это указывает на корректность сериализации/десериализации при соблюдении рекомендуемых процедур. Вместе с тем безопасность загрузки требует многоуровневого подхода: подпись и валидация артефактов, хеш-контроль, включение safe\_mode (с осознанием его ограничений), перенос только весов и использование weights\_only, а также аудит событий загрузки и ограничение источников моделей.

Таким образом, проверка SHA-256 и сравнение поведения подтверждают, что TensorFlow и PyTorch обеспечивают целостность и воспроизводимость модели при корректной эксплуатации. Для формирования доверенной цепочки поставок необходимо комбинировать цифровую подпись артефактов, хеш-контроль, безопасные режимы загрузки и операционные практики аудита, что в сумме снижает риск подмены и компрометации ML-моделей.

## СПИСОК ЛИТЕРАТУРЫ

1. Marusheak M., Wickens E. Launch of Model Signing v1.0: OpenSSF AI/ML Working Group Secures the Machine Learning Supply Chain // OpenSSF Blog. 2025-04-04. URL: <https://openssf.org/blog/2025/04/04/launch-of-model-signing-v1-0-openssf-ai-ml-working-group-secures-the-machine-learning-supply-chain/> (дата обращения: 10.07.2025).
2. Saini K. Hashing in Cyber Security: Understanding the Best Practices // Simplilearn. 2025-06-27. URL: <https://www.simplilearn.com/hashing-in-cybersecurity-article> (дата обращения: 12.07.2025).
3. TensorFlow Team. SavedModel // TensorFlow Core Guide. URL: [https://www.tensorflow.org/guide/saved\\_model](https://www.tensorflow.org/guide/saved_model) (дата обращения: 12.07.2025).
4. Polkovnichenko A. Is TensorFlow Keras “Safe Mode” Actually Safe? Bypassing safe\_mode Mitigation to Achieve Arbitrary Code Execution // JFrog Blog. 12.03.2025. URL: [https://jfrog.com/blog/keras-safe\\_mode-bypass-vulnerability/](https://jfrog.com/blog/keras-safe_mode-bypass-vulnerability/) (дата обращения: 15.07.2025).
5. PyTorch Team. Saving and Loading Models PyTorch Tutorials // PyTorch.org. URL: [https://docs.pytorch.org/tutorials/beginner/basics/saveloadrun\\_tutorial.html](https://docs.pytorch.org/tutorials/beginner/basics/saveloadrun_tutorial.html) (дата обращения: 16.07.2025).

УДК 621.391.3

## СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В ПРОГРАММНО-ОПРЕДЕЛЯЕМЫХ СЕТЯХ: АНАЛИЗ СОВРЕМЕННЫХ РЕШЕНИЙ, УГРОЗ И МЕТОДОВ ЗАЩИТЫ

Стародубцев Юрий Иванович, Митрофанов Михаил Валерьевич

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

Университет ИТМО

Кронверкский пр., 49, Санкт-Петербург, 197101, Россия

e-mails: prof.starodubtsev@gmail.com, vonafortim@andex.ru

**Аннотация.** Представлены результаты анализа функционирования систем обнаружения вторжений в программно-определяемых сетях. Описаны причины уязвимости архитектуры с разделением плоскости управления и плоскости передачи данных, основные типы атак на сеть (распределённый отказ в обслуживании, отказ в обслуживании, сканирование, внедрение вредоносных запросов к базам данных, эскалация привилегий и другие) и их последствия. Обобщены подходы к обнаружению вторжений: поиск известных шаблонов и выявление аномалий на основе статистических методов, методов машинного обучения и методов глубокого обучения. Отмечены ограничения существующих решений и обозначены направления практического применения и дальнейших исследований.

**Ключевые слова:** программно-определяемые сети; системы обнаружения вторжений; безопасность сетей; обнаружение аномалий; поиск по шаблонам; машинное обучение; глубокое обучение; распределённый отказ в обслуживании; канал связи между коммутатором и контроллером; аппаратные таблицы правил коммутатора.

## INTRUSION DETECTION SYSTEMS IN PROGRAM-DEFINED NETWORKS: ANALYSIS OF MODERN SOLUTIONS, THREATS, AND PROTECTION METHODS

Starodubtsev Yuri, Mitrofanov Mikhail

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

University ITMO

49 Kronverksky Av, St. Petersburg, 197101, Russia

e-mails: prof.starodubtsev@gmail.com, vonafortim@andex.ru



**Abstract.** The paper presents the results of an analysis of the functioning of intrusion detection systems in software-defined networks. It describes the causes of vulnerability in the architecture with a separation of the control plane and the data plane, the main types of network attacks (distributed denial of service, denial of service, scanning, injection of malicious database requests, privilege escalation, and others), and their consequences. The paper summarizes approaches to intrusion detection, including the search for known patterns and the detection of anomalies using statistical methods, machine learning methods, and deep learning methods. The limitations of existing solutions are noted, and directions for practical application and further research are outlined.

**Keywords:** software-defined networks; intrusion detection systems; network security; anomaly detection; pattern matching; machine learning; deep learning; distributed denial of service; communication channel between the switch and the controller; switch hardware rule tables.

*Постановка задачи.* Программно-определяемые сети упрощают управление трафиком: решения о маршрутизации и защите принимаются в одном центре, а устройства передачи данных реализуют эти решения. Такая архитектура удобна, но создаёт новые угрозы: перегрузка центрального узла управления, перехват и подмена правил, а также увеличение трафика между коммутатором и контроллером. Цель работы — понять, какие виды атак наиболее опасны и какие системы обнаружения вторжений реально помогают в современных условиях [1].

*Основные угрозы.* Наибольший ущерб вызывают массовые потоки вредоносного трафика, создаваемые с многих устройств одновременно, что приводит к распределённому отказу в обслуживании, а также целенаправленные действия по истощению ресурсов центрального узла управления. К частым угрозам относятся сканирование сети, внедрение вредоносных запросов к базам данных, удалённое получение локального доступа и повышение привилегий. Последствия — задержки и потери легитимного трафика, нарушение качества обслуживания и отказ критичных сервисов [2].

*Подходы к обнаружению вторжений.* Существуют два базовых подхода. Первый — поиск известных шаблонов вредоносной активности. Он даёт низкое число ложных тревог, но слабо защищает от новых атак. Второй — выявление аномалий: строится «нормальная» картина поведения сети и фиксируются отклонения. Для этого используют статистические методы, методы машинного обучения и методы глубокого обучения. Показатели качества обычно включают точность, полноту, точность положительных выявлений и обобщенный показатель [3].

*Ограничения и практические выводы.* Реальные сети работают на высоких скоростях, поэтому анализ трафика не должен перегружать центральный узел управления. Многие исследовательские наборы данных устарели и плохо отражают сегодняшние атаки и объёмы трафика. Нужны новые модели, которые с высокой достоверностью показывают, почему принято то или иное решение, и способны работать в реальном времени. На практике полезно распределять задачи обнаружения между центральным узлом управления и устройствами передачи данных, а также заранее ограничивать объём служебных запросов, чтобы защитить таблицы маршрутизации от засорения.

*Направления дальнейших исследований.* Следует создавать обновляемые наборы данных, отражающие современный сетевой трафик, и методики оценки, учитывающие задержки и потери. Перспективно проектировать совместно архитектуру сети и систему обнаружения: определять, какие проверки выполнять ближе к источнику трафика, а какие — в центре управления. Необходимо развивать методы анализа, чтобы специалисты могли доверять решениям системы обнаружения.

#### СПИСОК ЛИТЕРАТУРЫ

1. Y. Maleh, Y. Qasmaoui, K. El Gholami, Y. Sadqi, and S. Mounir, «Acomprehensive survey on SDN security: Threats, mitigations, and future directions» J. Reliable Intell. Environments, vol. 9, no. 2, pP. 201–239, Jun. 2023.
2. R. Palanikumar and K. Ramasamy, «Software dened network basedself-diagnosing faulty node detection scheme for surveillance applications» Comput. Commun., vol. 152, pP. 333–337, Feb. 2020.
3. A. Abdulghaffar, A. Mahmoud, M. Abu-Amara, and T. Sheltami, «Modeling and evaluation of software dened networking based 5G core network architecture» IEEE Access, vol. 9, pP. 10179–10198, 2021.

УДК 621.396.4

#### ИНТЕРВАЛЬНАЯ ОЦЕНКА КАЧЕСТВА УПРАВЛЕНЧЕСКИХ, МЕТОДИЧЕСКИХ И ПРАКТИЧЕСКИХ НАВЫКОВ ДОЛЖНОСТНЫХ ЛИЦ ОРГАНОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Шамиев Вячеслав Александрович, Пантюхин Олег Игоревич, Парашук Игорь Борисович

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: shamiev@list.ru, p\_oleg99@mail.ru, shchuk@rambler.ru

**Аннотация.** В докладе детально рассмотрены особенности современной формулировки сущности и содержания управленческих, методических и практических навыков должностных лиц органов информационной безопасности телекоммуникационных сетей. Предложен новый интервальный подход к прогнозированию текущих и прогностических оценок качества управленческих, методических и практических навыков, который позволяет, при его применении, повысить достоверность поддержки принятия решений по формированию новых

знаний и умений у специалистов такого класса. Изучены и проанализированы возможности использования алгоритмов интервальной оценки качества, приобретаемых специалистами управленческих, методических и практических навыков в рамках образовательной деятельности по подготовке инженерных кадров, нацеленных на эффективную защиту информации.

**Ключевые слова:** телекоммуникационная сеть; интервальная оценка; качество; информационная безопасность; навыки; обучение.

**INTERVAL ASSESSMENT OF THE QUALITY OF MANAGERIAL, METHODOLOGICAL  
AND PRACTICAL SKILLS OF OFFICIALS OF INFORMATION SECURITY BODIES  
OF TELECOMMUNICATION NETWORKS**

**Shamiev Vyacheslav, Pantyukhin Oleg, Parashchuk Igor**

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: shamiev@list.ru, p\_oleg99@mail.ru, shchuk@rambler.ru

**Abstract.** The report examines in detail the features of the modern formulation of the essence and content of managerial, methodological and practical skills of officials of information security agencies of telecommunication networks. A new interval approach to forecasting current and prognostic assessments of the quality of managerial, methodological and practical skills is proposed, which allows, when applied, to increase the reliability of decision-making support for the formation of new knowledge and skills in specialists of this class. The possibilities of using algorithms for interval assessment of the quality of managerial, methodological and practical skills acquired by specialists in the framework of educational activities for the training of engineering personnel aimed at effective information protection are studied and analyzed.

**Keywords:** telecommunication network; interval assessment; quality; information security; skills; training.

В современном сложном и максимально компьютеризированном мире огромное значение придается управленческим, методическим и практическим навыкам должностных лиц (ДЛ) органов информационной безопасности (ОИБ) телекоммуникационных сетей (ТКС).

При этом под управленческими, методическими и практическими навыками принято понимать компетенции, необходимые для эффективной работы ДЛ ОИБ ТКС в сферах менеджмента защищенности, обучения основам и принципам информационной безопасности и практике реализации политики безопасности на ТКС регионального либо федерального масштаба.

Иными словами, если рассматривать эти навыки как отдельные наборы знаний и умений, то управленческие навыки можно охарактеризовать как комплекс компетенций и способностей, необходимых для планирования, организации, мотивации и контроля работы ДЛ и процессов по обеспечению информационной безопасности в ТКС.

При этом к управленческим навыкам, необходимым специалистам для эффективной работы ДЛ ОИБ ТКС, можно отнести: навыки стратегического планирования — умение ДЛ ОИБ разрабатывать долгосрочные стратегии для достижения высокого уровня информационной безопасности ТКС, включая анализ и прогнозирование изменений; навыки управления проектами — способность ДЛ ОИБ планировать, организовывать и контролировать весь цикл выполнения проектов по обеспечению (достижению) высокого уровня информационной безопасности ТКС, включая управление ресурсами, сроками и финансами; навыки лидерства — способность ДЛ ОИБ вдохновлять и мотивировать команду, устанавливать четкие и достижимые цели; навыки по разрешению конфликтов — способность ДЛ ОИБ выявлять и управлять конфликтами, позволяющая эффективно находить компромиссы при решении задач по обеспечению (достижению) высокого уровня информационной безопасности ТКС; навыки управления временем — способность ДЛ ОИБ к организации и ранжированию приоритетов при распределении времени на решение задач по обеспечению (достижению) высокого уровня информационной безопасности ТКС, по для повышению продуктивности средств и комплексов защиты информации на объектах такого класса; навыки критического мышления — умение ДЛ ОИБ критически анализировать информацию, что помогает принимать обоснованные и взвешенные решения по достижению высокого уровня информационной безопасности ТКС.

К методическим навыкам, необходимым, в частности, для обучения специалистов ОИБ ТКС, можно отнести умения, связанные, например, с организацией учебного процесса, процедур и алгоритмов обучения должностных лиц ОИБ объектов такого класса: навыки методического анализа учебного материала, необходимого для организации учебного процесса, процедур и алгоритмов обучения должностных лиц ОИБ ТКС; навыки перспективного и текущего планирования системы занятий по теоретическому и практическому обучению, по установлению межпредметных связей при организации учебного процесса, процедур и алгоритмов обучения должностных лиц ОИБ ТКС; навыки разработки содержания коллективных, групповых и индивидуальных форм работы учащихся на занятиях по обучению основам и принципам информационной безопасности; навыки разработки недостающих средств обучения (учебно-методических пособий, частных методик, конспектов лекций) для занятий по обучению основам и принципам информационной безопасности, а также навыки моделирования и конструирования форм предъявления учебной информации на занятиях по обучению основам и принципам информационной безопасности в ТКС.

К практическим навыкам, жизненно необходимым специалистам для эффективной работы ДЛ ОИБ ТКС, можно отнести их умения применять теоретические знания на практике. Они помогают: развить навыки анализа, выявления и обеспечения решения проблем информационной безопасности телекоммуникационных сетей; подготовиться к реальным практическим ситуациям, с которыми можно столкнуться в профессиональной деятельности ДЛ ОИБ ТКС; понять, как работают различные инструменты и методы обеспечения информационной безопасности, а также как их можно использовать для защиты ТКС.

При этом к базовым направлениям практических навыков, необходимых ДЛ ОИБ ТКС, относят: навыки по применению методов обнаружения и предотвращения атак, по анализу уязвимостей сетевой инфраструктуры; навыки в криптографии — умения применять алгоритмы шифрования, дешифрования, методы аутентификации и цифровой подписи; навыки управления безопасностью информации на ТКС — умения ДЛ по разработке и внедрению политик и процедур, направленных на обеспечение конфиденциальности, целостности и доступности информации; навыки по разработке и тестированию систем защиты информации, например, программ для шифрования данных или управления доступом пользователей ТКС, а также навыки по web-разработке и обеспечению безопасности приложений, умения создавать и тестировать защищенных web-приложения и сайты, которые устойчивы к кибератакам на телекоммуникационную сеть.

Воплощение в жизнь процедур текущего и прогностического, упреждающего контроля качества управленческих, методических и практических навыков ДЛ ОИБ ТКС является предметом, а сами навыки — объектом исследований, при этом практики признают, что используемые ныне подходы к анализу и прогнозу качества подобных навыков, не соответствуют современным требованиям.

Рациональным, по нашему мнению, подходом (способом) к решению данной проблемы, может стать использование алгоритмов математического анализа интервальных средних, позволяющих получать усредненные за интервал времени текущие и прогностические оценки уровня навыков, получать интервальные (пороговые по верхней и по нижней границе значений) оценки показателей качества управленческих, методических и практических навыков ДЛ ОИБ ТКС [1-5].

Специфика подобного подхода (способа), определяющая его новизну, заключается в наличии в его составе специального алгоритма для получения усредненных за интервал времени текущих и прогностических оценок качества управленческих, методических и практических навыков ДЛ ОИБ ТКС, которые могут быть описаны с помощью случайных событий, например, текущих и прогностических оценок.

Подход (способ), ориентированный на получение интервальных текущих и прогностических оценок качества управленческих, методических и практических навыков ДЛ ОИБ ТКС, позволяет осуществлять не только расчет экстраполированных значений показателей качества подобных навыков, но и оповещать администратора (пользователя) о получении потенциально опасных оценочных данных.

Таким образом, предложен новый методологический подход (способ) для прогнозирования усредненных за интервал времени текущих и прогностических оценок качества управленческих, методических и практических навыков ДЛ ОИБ ТКС, который позволяет, при его применении, повысить достоверность поддержки принятия решений по формированию новых знаний и умений у обучаемых преподавательским составом в рамках образовательной деятельности, позволяет избежать критических ошибок при комплектовании учебных программ по обучению специалистов в сфере информационной безопасности телекоммуникационных сетей.

#### СПИСОК ЛИТЕРАТУРЫ

1. Лемешко Б.Ю., Постовалов С.Н. О решении задач статистического анализа интервальных наблюдений // Вычислительные технологии. Т.2. Новосибирск: 1997. С. 28-36.
2. Гуров С.В., Уткин Л.В., Надежность систем при неполной информации. СПб.: Любавич, 1999. 160 с.
3. Крюкова Е.С. Модели и методы интервальной оценки качества электронных библиотек и контента электронных образовательных ресурсов: Монография. СПб.: ВАС, 2025. 108 с.
4. Парашук И.Б. Информационная безопасность телекоммуникационной компоненты киберфизических систем // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 4 / СПОИСУ. СПб.: 2017. С. 150-152.
5. Парашук И.Б., Крюкова Е.С. Превентивный интервальный контроль качества систем хранения и обработки электронных образовательных ресурсов на основе моделирования и прогнозирования случайных событий // Инновационная деятельность в Вооруженных Силах Российской Федерации: Труды всеармейской научно-практической конференции. 12-13 октября 2023 года, СПб.: ВАС, 2023. С. 593-598.

УДК 681.322.067

#### РАЗРАБОТКА АНАЛИТИЧЕСКОГО АППАРАТА ДЛЯ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПРИ ПЛАНИРОВАНИИ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

Шарко Геннадий Васильевич<sup>1</sup>, Шарко Тамара Валентиновна<sup>2</sup>

<sup>1</sup>Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

<sup>2</sup>Средняя образовательная школа № 197

Фурштадтская ул., 29А, Санкт-Петербург, 191123, Россия

e-mails: shgorg@mail.ru, t.v.sharko.19@gmail.com

**Аннотация.** В статье рассмотрены полученные в ходе исследований расчетные соотношения для оценки нагрузочных (максимальной обслуживаемой КМД нагрузки) и структурных (максимально допустимого количества корреспондентов в КМД) параметров, учитывающие энергетические соотношения сигналов

корреспондентов, функционирующих в КМД, полученные выражения позволяют оценить нагрузочные и структурные параметры КМД, в том числе, через энергетические характеристики сигналов корреспондентов. Применение данного математического аппарата в составе специального программного обеспечения (СПО) комплексов технических средств передачи данных (КСТПД) позволит в реальном масштабе времени адаптировать СОД с динамической структурой к изменениям ее характеристик. Тем самым будут обеспечены более эффективное распределение ресурсов КМД, снижение непроизводительных потерь ресурсов, и, как следствие, повышение пропускной способности СОД в целом.

**Ключевые слова:** канал множественного доступа (КМД); внешние помехи; внутрисистемные помехи; необнаруживаемый конфликт; соотношение сигнал-шум; контроль занятости канала; максимальная обслуживаемая нагрузка; максимально допустимое количество корреспондентов в КМД; система обмена данными (СОД).

## DEVELOPMENT OF AN ANALYTICAL APPARATUS FOR DECISION SUPPORT SYSTEMS IN PLANNING DATA TRANSMISSION NETWORKS

Sharko Gennady<sup>1</sup>, Sharko Tamara<sup>2</sup>

<sup>1</sup>The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny  
3 Tikhoretsky Av, St. Petersburg, 194064, Russia

<sup>2</sup>Secondary educational school No 197  
29A Furshtadtskaya St., Saint Petersburg, 191123, Russia  
e-mails: shgorg@mail.ru, t.v.sharko.19@gmail.com

**Abstract.** The article considers the calculated ratios obtained in the course of research to estimate the load (maximum load serviced by the KMD) and structural (maximum allowable number of correspondents in the KMD) parameters, taking into account the energy ratios of the correspondents' signals operating in the KMD. The expressions obtained allow us to estimate the load and structural parameters of the KMD, including through the energy characteristics of the correspondents' signals. The use of this mathematical apparatus as part of special software (SPO) of data transmission technology complexes (CCTPS) will make it possible to adapt ODS with a dynamic structure to changes in its characteristics in real time. This will ensure a more efficient allocation of KMD resources, a reduction in unproductive resource losses, and, as a result, an increase in the capacity of the SOD as a whole.

**Keywords:** multiple access channel (KMD); external interference; in-system interference; undetectable conflict; signal-to-noise ratio; channel occupancy control; maximum serviced load; maximum allowable number of correspondents in KMD; data exchange system (DMS).

В условиях ускоряющегося развития и совершенствования систем обмена данными становится очевидным, что эффективное распределение их ресурсов и, следовательно, их характеристики становятся все более зависимыми от правильной и своевременной оценки ситуаций в сетях и системах [1–3]. Используемые в настоящее время алгоритмы множественного доступа, в которых не используются количественные оценки КМД как результат применения прикладных расчетных задач, обладают недостаточной степенью адаптации к воздействию внешних и внутрисистемных помех и не позволяют эффективно использовать энергетические и частотные ресурсы СОД.

Статья посвящена отысканию подходов к моделированию КМД на базе радиоканала, которая, при реализации ее в СПО КСТПД СОД в качестве аппарата решения расчетных задач по планированию сетей передачи данных, позволит повысить эффективность управления КМД и СОД в целом. Для группы корреспондентов, являющихся источниками и потребителями информации, выделена группа рабочих частот (при этом количество выделенных частот значительно меньше организуемых в группе радионаправлений). Каждая из выделенных частот используется парой корреспондентов только на время проведения сеанса связи, а затем освобождается. В силу особенностей пространственного размещения корреспондентов, их стохастического перемещения и случайного характера энергетических соотношений сигналов корреспондентов и поступающей от них нагрузки возможно одновременное использование выделенных частот несколькими парами корреспондентов (то есть возникновение конфликтов).

При допущении отсутствия внешних помех для радиосети внутрисистемные помехи, вызванные одновременным использованием одной и той же рабочей частоты двумя и более корреспондентами, приводят к проявлению некоторых специфических особенностей КМД.

Пусть какой-либо корреспондент выбирает частоту, на которой уровень помех меньше заданного порогового значения. При этом вокруг данного корреспондента образуется ряд зон, обусловленных пространственно-энергетическими характеристиками КМД.

Первая зона является зоной обнаружения чужой передачи и блокирования собственной (зоной обнаружения конфликта). Вторая зона — это зона возникновения необнаруживаемого конфликта двух и более корреспондентов из-за большого расстояния между корреспондентами (что приводит к невозможности определения факта чужой передачи из-за конечного времени распространения сигнала).

Третья зона — это зона возникновения необнаруживаемого конфликта из-за пониженных энергетических характеристик сигнала передающего корреспондента. Четвертая зона является зоной связи, в которой возможно

повторное использование частоты, занятой передающим корреспондентом, так как данная частота при анализе состояния канала оценивается как незанятая (свободная).

В первой зоне уровень мешающего сигнала от передающего корреспондента превышает заданное пороговое значение помехи для всех корреспондентов в данной зоне, что приводит к невозможности занятия анализируемой частоты другим корреспондентом из-за занятия ее передающим корреспондентом. Таким образом, граница этой зоны определяется уровнем сигнала передатчика передающего корреспондента, который является помехой для других корреспондентов данной радиосети, пытающихся использовать эту же частоту. Вместе с тем незначительное взаимное удаление корреспондентов позволяет четко идентифицировать передачу пакета корреспондентом «своей» радиосети и блокировать собственную передачу в момент обнаружения занятия КМД (что устраняет возможность возникновения конфликта и тем самым повышает пропускную способность КМД). Это обеспечивается реализацией алгоритма случайного множественного доступа с контролем занятости канала (МДКЗ) с использованием анализатора занятости канала [4]. В качестве признака занятости канала в данном случае используется наличие в нем сигналов, структура которых соответствует кодовым комбинациям используемого помехоустойчивого кода. При обнаружении в канале заданного количества следующих подряд кодовых комбинаций с необнаруженными ошибками вырабатывается сигнал о занятости канала и вводится временная блокировка, в течение которой запрещается передача сообщений в канал. Выход из состояния блокировки происходит через определенный интервал времени, отсчитываемый с момента формирования последнего сигнала о занятости канала.

Во второй зоне с увеличением взаимного удаления корреспондентов вероятность возникновения конфликта возрастает, но энергетические характеристики сигнала передающего корреспондента еще заставляют некоторых корреспондентов сети оценивать данную частоту как занятую.

В третьей зоне возможны конфликты из-за взаимных помех, создаваемых другими корреспондентами радиосети, которые оценивают данную частоту как свободную и пытаются использовать ее для установления связи.

Полученные в ходе исследований расчетные соотношения для основных нагрузочных и структурных параметров КМД с учетом энергетических характеристик сигналов корреспондентов КМД в дальнейшем будут использованы при разработке модели КМД на базе радиоканала, которая, при реализации ее в СПО КТСРД СОД в качестве аппарата решения прикладных расчетных задач по планированию сетей передачи данных, позволит повысить эффективность управления КМД и СОД в целом.

#### СПИСОК ЛИТЕРАТУРЫ

1. Росляков А.В., Герасимов А.В. Детерминированные сети связи и их стандартизация. // Стандарты и качество. 2024. № 7. С. 42–47.
2. Гезалов Э.Б. Модель неоднородной локальной сети связи с протоколом синхронного временного доступа с учетом надежности ее элементов // Т-Comm: Телекоммуникации и Транспорт. 2021. Т. 15. № 3. С. 25–29.
3. Верзун Н.А., Воробьев А.И., Пойманова Е.Д. Моделирование процесса передачи информации с разграничением прав доступа пользователей // Известия высших учебных заведений. Приборостроение. 2014. Т. 57. № 9. С. 33–37.
4. Верзун Н.А., Колбанёв М.О., Советов Б.Я. Корпоративный алгоритм множественного доступа в киберпространстве. Труды учебных заведений связи. 2025;11(3):97-107.



## ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

УДК 004.056:338.1

### ВЛИЯНИЕ ИМПОРТОЗАМЕЩЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА УРОВЕНЬ ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ

**Аминов Хакимджон Иномджонович, Лескова Елизавета Михайловна**

Санкт-Петербургский государственный экономический университет  
Канала Грибоедова наб., 30-32, лит. А, Санкт-Петербург, 191023, Россия  
e-mails: h\_aminov@unecon.ru, liza.leskova2004@gmail.com

**Аннотация.** Исследована проблема импортозамещения программного обеспечения в российской промышленности как ключевого фактора информационно-экономической безопасности. Анализ показал значительную зависимость промышленных предприятий от зарубежного программного обеспечения. Определены основные группы рисков перехода на отечественное программное обеспечение: технические, кадровые и экономические. Обоснована необходимость комплексного подхода, включающего оценку функциональной зрелости отечественного программного обеспечения, анализ кадрового потенциала и расчет совокупной стоимости владения.

**Ключевые слова:** промышленные предприятия; информационно-экономическая безопасность; импортозамещение программного обеспечения; риски перехода; отечественное программное обеспечение.

### THE IMPACT OF SOFTWARE IMPORT SUBSTITUTION ON THE LEVEL OF INFORMATION AND ECONOMIC SECURITY OF INDUSTRIAL ENTERPRISES

**Aminov Khakimdzhon, Leskova Elizaveta**

St. Petersburg State University of Economics  
30-32 Griboedov Channel Emb, St. Petersburg, 191023, Russia  
e-mails: h\_aminov@unecon.ru, liza.leskova2004@gmail.com

**Abstract.** The problem of software import substitution in the Russian industry has been studied as a key factor in information and economic security. The analysis showed a significant dependence of industrial enterprises on foreign software. The main groups of transition risks have been defined: technical, personnel, and economic. The necessity of a comprehensive approach has been justified, which includes assessing the functional maturity of the domestic software, analyzing human resources potential, and calculating the total cost of ownership.

**Keywords:** industrial enterprises; information and economic security; import substitution of software; transition risks; domestic software.

Актуальность исследования обусловлена тем, что несмотря на объективную потребность в импортозамещении программного обеспечения (ПО), сохраняется дефицит исследований, посвящённых анализу баланса между достижением технологической независимости и управлением возникающими рисками.

Вследствие интенсивной цифровизации промышленности возникла критическая зависимость предприятий от ПО, ставшего ключевым элементом обеспечения информационно-экономической безопасности [1]. Уход иностранных поставщиков программного обеспечения и санкционное давление повлекли за собой увеличение уязвимости организаций, использующих зарубежные программные продукты. По данным исследований «K2Tex» и Arenadata за 2024 год, лишь 22% промышленных предприятий достигли высокого уровня замещения программного обеспечения, в то время как у 78% компаний доля внедрённого отечественного ПО не превышает 70%, что свидетельствует о значительной доле присутствия зарубежного ПО в критических процессах предприятий [2, 3]. Процесс перехода на отечественные решения в целях достижения технологического суверенитета сопровождается возникновением новых угроз [4–6].

Преимущества использования отечественных цифровых технологий заключаются в том, что они способствуют обеспечению информационной безопасности и экономической независимости от иностранных поставщиков [7], уменьшая вероятность внезапных отключений лицензий, отказов в обновлениях и сервисной поддержке. Также импортозамещение служит основой для формирования новой отрасли производства в стране [7]. Особенно это актуально в условиях санкций и геополитической напряжённости, когда доступ к зарубежному ПО и его сопровождению может быть ограничен, что отражается на стабильности и безопасности критически важных процессов на промышленных предприятиях.

Негативные аспекты импортозамещения связывают с несколькими ключевыми группами рисков. Первая группа — технические риски, вызванные недостаточной развитостью части отечественного программного обеспечения. Нередко российские аналоги зарубежных систем не отвечают международным стандартам качества, что ограничивает их применение в высокотехнологичных отраслях и может привести к потере рыночной доли и снижению конкурентоспособности. Вторая группа — кадровые риски, связанные с дефицитом квалифицированных специалистов, способных администрировать и эксплуатировать отечественные решения. Это может приводить к снижению качества сопровождения IT-инфраструктуры и замедлению внедрения отечественных технологий. Третья группа — экономические риски, обусловленные высокими затратами, необходимыми для модернизации производства [4].

Импортозамещение программного обеспечения в промышленности необходимо рассматривать не просто как технологическую замену, а как комплексный проект по управлению информационными рисками, напрямую влияющий на устойчивость и конкурентоспособность бизнеса. Системное внедрение отечественных цифровых решений должно сопровождаться глубоким анализом как технических, так и экономических последствий, а также организационных факторов, что позволит минимизировать возникающие угрозы и максимально использовать потенциал импортозамещения.

Для эффективной реализации данной стратегии целесообразно сфокусироваться на трёх ключевых аспектах.

1. Анализ функциональной зрелости и соответствия отечественного ПО международным стандартам качества, направленный на выявление потенциальных пробелов в функционале, производительности и безопасности.

2. Оценка кадрового потенциала и кадровых рисков, включающая аудит наличия квалифицированных специалистов для внедрения и сопровождения новых систем, а также разработку программ переподготовки и адаптации моделей удержания ключевых кадров, что позволит избежать снижения качества IT-инфраструктуры.

3. Анализ совокупной стоимости владения при переходе на отечественное программное обеспечение, который позволит предприятиям более точно планировать бюджет и избегать неожиданных финансовых потерь.

4. Можно сделать вывод, что процесс импортозамещения программного обеспечения в промышленности представляет собой сложную многогранную проблему, непосредственно влияющую на обеспечение информационно-экономической безопасности предприятий.

5. Для успешной реализации стратегии импортозамещения необходима разработка комплексных методик оценки, учитывающих не только нормативные требования, но и весь спектр возникающих рисков. Такой подход позволит сформировать сбалансированную модель цифровой трансформации, обеспечивающую как технологический суверенитет, так и устойчивое развитие промышленных предприятий.

#### СПИСОК ЛИТЕРАТУРЫ

1. Колбанёв М.О., Коршунов И.Л., Левкин И.М. Информатизация и информационно-экономическая безопасность // Россия и Санкт-Петербург: экономика и образование в XXI веке: научная сессия профессорско-преподавательского состава, научных сотрудников и аспирантов по итогам НИР за 2015 год. Март-апрель 2016 года: Сборник лучших докладов. СПб.: Изд-во СПбГЭУ, 2016. С. 159-163.
2. Только 22% промышленных компаний заменили ПО для работы с данными более чем на 70% // K2TEX: сайт. URL: [https://k2.tech/press\\_releases/22-prochenta-promyshlennyh-kompanij-zamestili-po-dlya-raboty-s-dannymi/](https://k2.tech/press_releases/22-prochenta-promyshlennyh-kompanij-zamestili-po-dlya-raboty-s-dannymi/) (дата обращения: 20.08.2025).
3. Читанова В. Импортозамещение промышленного ПО: где и как идет замена // Коммерсантъ: сайт. URL: <https://www.kommersant.ru/doc/7738015> (дата обращения: 20.08.2025).
4. Аминов Х.И., Ануфриев М.С. Актуальные вопросы управления предпринимательскими рисками цифровой трансформации // Экономика и управление: проблемы, решения. 2023. Т. 2, № 6(138). С. 46-54. DOI 10.36871/ek.up.p.g.2023.06.02.005.
5. Аминов Х.И., Дремезова А.А. Опасности цифровой среды для бизнеса и общества // Цифровые опасности информационного общества: Сборник статей / Под редакцией И.Л. Коршунова. СПб.: Изд-во СПбГЭУ, 2023. С. 20-29.
6. Бондаренко Д.В., Громова Н.В. Импортозамещение в промышленности как фактор обеспечения экономической безопасности в условиях отрицательного проявления глобализации // Индустриальная экономика. 2025. № 2. С. 31-37. DOI 10.47576/2949-1886.2025.2.2.004.
7. Якушев Н.О., Устинова К.А., Кочнев А.А. Импортозамещение как фактор развития отечественных цифровых технологий // Экономические и социальные перемены: факты, тенденции, прогноз. 2024. Т. 17, № 3. С. 82-101. DOI 10.15838/esc.2024.3.93.5.

УДК 004.056:338.43

#### ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ АПК В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ НА ПРИМЕРЕ КРАСНОДАРСКОГО КРАЯ

**Аминов Хакимджон Иномджонович, Семиколенных Владимир Викторович**

Санкт-Петербургский государственный экономический университет  
Канала Грибоедова наб., 30-32, лит. А, Санкт-Петербург, 191023, Россия  
e-mails: h\_aminov@unecon.ru, semka1965@bk.ru

**Аннотация.** Исследована проблема уязвимости цифровой инфраструктуры агросектора Краснодарского края в условиях активной цифровой трансформации. Обнаружены новые угрозы: рост числа кибератак, зависимость от зарубежных технологий и дефицит кадров. Предложены меры по обеспечению информационно-экономической безопасности, включая импортозамещение, защиту цифровой инфраструктуры и подготовку специалистов. Сделан вывод о необходимости комплексного подхода для устойчивого развития и продовольственной безопасности региона.

**Ключевые слова:** цифровая трансформация; агропромышленный комплекс; Краснодарский край; информационно-экономическая безопасность; киберугрозы.

**INFORMATION AND ECONOMIC SECURITY OF THE AGRO-INDUSTRIAL COMPLEX  
IN THE CONTEXT OF DIGITAL TRANSFORMATION ON THE EXAMPLE  
OF THE KRASNODAR TERRITORY APPLICATION**

**Aminov Khakimdzhon, Semikolennykh Vladimir**

St. Petersburg State University of Economics

30-32 Griboedov Channel Emb, St. Petersburg, 191023, Russia

e-mails: h\_aminov@unecon.ru, semka1965@bk.ru

**Abstract.** The article deals with the vulnerability of the digital infrastructure of the agricultural sector of the Krasnodar Territory in the context of active digital transformation. New threats have been identified: an increase in the number of cyberattacks, dependence on foreign technologies and a shortage of personnel. Information and economic security measures are proposed, including import substitution, protection of digital infrastructure and training of specialists. It is concluded that an integrated approach is necessary for the sustainable development and food security of the region.

**Keywords:** digital transformation; agricultural sector; Krasnodar Region; information and economic security; cyber threats.

В настоящее время Краснодарский край занимает лидирующую позицию среди регионов по производству сельскохозяйственной продукции. Данный сектор активно модернизируется с 2023 года за счёт внедрения современных технологий, среди которых: дроны, автоматизированные системы, методы точного земледелия и цифровые логистические платформы. По данным Минсельхоза, в 2024 году более 60% крупных и средних хозяйств региона пользовались технологиями точного земледелия (спутниковый мониторинг, дроны, датчики влажности и плодородия). Это позволило повысить урожайность на 15-20% и снизить издержки на транспортировку [1]. В регион активно приходят роботизированные системы и цифровые платформы. Современные комбайны и тракторы оснащаются системами автопилота, а в животноводстве появляются «умные фермы» с датчиками контроля состояния животных [2]. Кроме того, Минсельхоз России реализует проект по созданию единой цифровой платформы государственных услуг в АПК, что должно охватить весь цикл — от мониторинга полей до экспорта готовой продукции [3]. Внедрение искусственного интеллекта и больших данных также становится заметным трендом. Данные нововведения позволяют прогнозировать урожайность, оптимизировать логистику и снизить потери на всех этапах производства, что повышает экономическую эффективность и качество продукции. Всё это значительно повышает эффективность работы, однако технологический прогресс также создаёт новые уязвимости, которые могут снизить уровень информационно-экономической безопасности.

Интенсивная цифровая трансформация приводит к появлению новых рисков, включая повышенную вероятность целевых кибератак, инцидентов, связанных с утечкой данных, и возрастающую уязвимость цепочек поставок [4–6]. В 2024 году Positive Technologies зафиксировала рост числа критических уязвимостей в отечественном программном обеспечении (ПО) на 39% по сравнению с 2023 годом [7], что напрямую отражается на безопасности агросектора.

Уязвимость ПО может привести к серьёзным проблемам. Сбои в системах мониторинга или логистики могут привести к остановке сбора урожая и экономическим потерям. Утечка данных о прогнозах урожайности и объёмах экспорта может негативно сказаться на ценах и международных поставках, ведь эта информация имеет стратегический характер. Дополнительным риском остаётся зависимость от зарубежных решений: значительная часть программного обеспечения и аналитических сервисов всё ещё основана на иностранных технологиях. В условиях санкций это создаёт угрозу отключения и потери доступа к критически важным сервисам. Не менее значимой проблемой является нехватка кадров. Цифровизация требует специалистов нового профиля — операторов дронов, агроаналитиков, специалистов по информационной безопасности. Их пока недостаточно, и этот дефицит тормозит развитие отрасли. Разрыв наблюдается и между крупными агрохолдингами и малыми хозяйствами: если первые уже активно внедряют дроны, интернет вещей и искусственный интеллект, то вторые зачастую ограничиваются базовой автоматизацией из-за высокой стоимости решений и нехватки субсидий.

Среди самых крупных кибератак на АПК за последнее время в России можно выделить кибератаку на АО Фирма «Агрокомплекс им. Ткачева», которая привела к техническому сбою всех ИТ-систем компании [8], атаку на агрохаб «Селятино», где злоумышленники вмешались в систему холодильного оборудования и едва не испортили 40 тысяч тонн продукции [9]. Шифровальщики также выводили из строя электронный документооборот в крупных холдингах — например, «Мираторг», что негативно сказалось на логистике и ветеринарном сопровождении грузов [10].

Справляться с этими вызовами можно лишь комплексно. Прежде всего требуется формирование защищённой цифровой инфраструктуры: внедрение шифрования данных, многофакторной аутентификации, проведение регулярных аудитов киберрисков.

Важную роль играет и импортозамещение — развитие отечественных дронов, датчиков, аналитических платформ. Примером инфраструктурного решения национального уровня является проект «Бюро 1440»,



предполагающий создание российской спутниковой группировки для обеспечения устойчивого интернет-покрытия в стране [11]. Это позволит использовать цифровые технологии даже в самых удалённых хозяйствах. Наконец, ключевым условием остаётся подготовка кадров: развитие программ цифровой грамотности для агрономов и операторов техники, открытие новых образовательных курсов и специализированных направлений в университетах региона.

Цифровизация агросектора в Краснодарском крае приносит заметные выгоды: рост эффективности, прозрачность логистики и снижение издержек. Однако на фоне усиления угроз критически важно для построения устойчивой цифровой экосистемы применять меры:

1. Разработка интегрированных стратегий информационно-экономической безопасности, охватывающих автоматизированные системы управления, облака, интернет вещей и другие системы. Информационная и экономическая безопасность должны работать как единое целое.

2. Регулярные аудит безопасности, особенно у подрядчиков. Ограничение доступа, сегментация сетей.

3. Обучение работников агросектора — не только ИТ-специалистов, но и операторов — основам безопасной работы с технологическими системами.

4. Постоянный мониторинг подозрительных действий в промышленной сети и выявление аномалий, особенно целенаправленных атак.

Такая комплексная политика позволит агропредприятиям защитить свои процессы, данные и логистику, сохранив динамику цифровизации без ущерба для безопасности и продовольственной устойчивости.

#### СПИСОК ЛИТЕРАТУРЫ

1. Журавлев Н. Цифра на грядке // Вестник АПК: сайт. URL: <https://vestnikapk.ru/articles/aktualno/tsifra-na-gryadke/> (дата обращения: 27.08.2025).
2. Цифровизация АПК помогает сократить затраты аграриев и повысить урожайность // СпецАгро: сайт. URL: <https://specagro.ru/news/202506/cifrovizaciya-apk-pomogaet-sokratit-zatraty-agrariyev-i-povysit-urozhaynost> (дата обращения: 28.08.2025).
3. Минсельхоз России формирует единую цифровую платформу АПК // Министерство сельского хозяйства РФ: официальный сайт. URL: <https://mcx.gov.ru/press-service/news/minselkhoz-rossii-formiruet-edinuyu-tsifrovuyu-platformu-apk/> (дата обращения: 28.08.2025).
4. Аминов Х.И., Ануфриев М.С. Актуальные вопросы управления предпринимательскими рисками цифровой трансформации // Экономика и управление: проблемы, решения. 2023. Т. 2, № 6(138). С. 46-54. DOI 10.36871/ek.up.p.r.2023.06.02.005.
5. Аминов Х.И., Дремезова А.А. Опасности цифровой среды для бизнеса и общества // Цифровые опасности информационного общества: Сборник статей / Под редакцией И.Л. Коршунова. СПб.: Изд-во СПбГЭУ, 2023. С. 20-29.
6. Модели цифровой опасности в кибернетическом и когнитивном пространствах: коллективная монография / под ред. М.О. Колбанёва, И.Л. Коршунова. СПб.: Изд-во СПбГЭУ, 2023. 194 с.
7. Софт уязвим, железо крепчает: прогнозы кибербезопасности-2025 // SecurityLab: сайт. URL: <https://www.securitylab.ru/news/555053.php> (дата обращения: 29.08.2025).
8. В Краснодарском крае зафиксированы кибератаки на крупнейшие агрохолдинги // РБК Краснодар: сайт. URL: <https://kuban.rbc.ru/krasnodar/freenews/661688a99a7947a1d3ca2d69> (дата обращения: 29.08.2025).
9. Anonymous пытались испортить 40 000 тонн продукции в агрохолдинге Селятино // SecurityLab: сайт. URL: <https://www.securitylab.ru/news/530388.php> (дата обращения: 29.08.2025).
10. Крупнейший в России агрохолдинг подвергся атаке шифровальщика // SecurityLab: сайт. URL: <https://www.securitylab.ru/news/530695.php> (дата обращения: 29.08.2025).
11. Создание российского аналога Starlink оценили почти в \$445 млрд // РБК: сайт. URL: [https://www.rbc.ru/technology\\_and\\_media/17/09/2024/66e8671f9a79472a671f62eb](https://www.rbc.ru/technology_and_media/17/09/2024/66e8671f9a79472a671f62eb) (дата обращения: 29.08.2025).

УДК 004.056

#### ВЛИЯНИЕ МЕРОПРИЯТИЙ ПО КИБЕРБЕЗОПАСНОСТИ НА ЭКОНОМИЧЕСКУЮ УСТОЙЧИВОСТЬ КОМПАНИИ

Андреевский Игорь Леонидович<sup>1</sup>, Кузнецова Ольга Борисовна<sup>2</sup>

<sup>1</sup> Санкт-Петербургский государственный экономический университет,  
Канала Грибоедова наб., 30-32, лит. А, Санкт-Петербург, 191023, Россия

<sup>2</sup> Мурманский арктический университет  
Спортивная, ул., 13, Мурманск, 183010, Россия  
e-mails: ail@unecon.ru, kuznetsovaob@mauniver.ru

**Аннотация.** Произведен анализ статистики киберпреступлений за 2004 год и первое полугодие 2025 года. Обоснована необходимость оценки эффективности мероприятий в области кибербезопасности. Предложены критерии, по которым должны формулироваться метрики и KPI.

**Ключевые слова:** оценка кибербезопасности; эффективность кибербезопасности; киберпреступления; метрики кибербезопасности; KPI кибербезопасности, ИТ-инфраструктура.

#### THE IMPACT OF CYBERSECURITY MEASURES ON THE ECONOMIC STABILITY OF A COMPANY

Andreevskiy Igor<sup>1</sup>, Kuznetsova Olga<sup>2</sup>

<sup>1</sup> St. Petersburg State University of Economics  
30-32 Griboedov Channel Emb, St. Petersburg, 191023, Russia

<sup>2</sup> Murmansk Arctic University,  
13 Sportivnaya St, Murmansk, 183010, Russia  
e-mails: ail@unecon.ru, kuznetsovaob@mauniver.ru

**Abstract.** An analysis of cybercrime statistics for 2004 and the first half of 2025 was conducted. The need to assess the effectiveness of cybersecurity measures was substantiated. Criteria were proposed for formulating metrics and KPIs.

**Keywords:** cybersecurity assessment; cybersecurity effectiveness; cybercrime; cybersecurity metrics; cybersecurity KPIs; IT infrastructure.

В современных условиях развития ИТ приходится констатировать рост киберпреступлений, совершаемых с их помощью. По словам статс-секретаря — замминистра цифрового развития РФ Ивана Лебедева, в 2024 году было совершено на 34,8% больше преступлений в сфере ИТ, чем в 2023 году, а общий ущерб составил не менее 160 млрд. руб., а по некоторым оценкам и того больше — примерно 250 млрд. руб. [1].

По статистике, в 2024 году киберпреступления составили 40% от общего числа зарегистрированных в стране преступлений — и это максимум с 2020 года и дальнейший рост продолжается. За первые 7 месяцев 2025 года доля киберпреступлений уже составила 38,9%, а общий ущерб по предварительным оценкам достиг величины в 119,6 млрд. руб. [2].

По данным исследователей, за 2024 год количество заказных кибератак, направленных на российские компании, увеличилось более чем в четыре раза.

Следовательно, необходима постоянная оценка уровня кибербезопасности, т.е. наличие четкого набора метрик и ключевых показателей эффективности (KPI), которые помогут компаниям оценить эффективность предпринимаемых ими мер кибербезопасности и, как следствие, принимать обоснованные решения.

Правильно подобранные и постоянно отслеживаемые метрики и ключевые показатели эффективности (KPI) помогут отследить влияние киберугроз на прибыль компании, ее репутацию и соответствие требованиям кибербезопасности. KPI являются эффективным способом оценки результативности и степени достижения поставленных целей, а, следовательно, помочь в принятии решений.

KPI обычно формулируются исходя из ключевых показателей кибербезопасности, имеющих первостепенное значение для руководителей компаний, для которых важна реализации бизнес-стратегии и инвестиции. К ним в первую очередь можно отнести стоимость киберинцидентов, снижение риска с течением времени, соблюдение нормативных требований, автоматизация реагирования на инциденты, управление рисками поставщиков [3].

Исходя из этих критериев компании формируют состав показателей, благодаря которым можно определить текущий уровень кибербезопасности и способы его оценки.

Таким образом, оценка эффективности мероприятий в области кибербезопасности оценивается по таким показателям, как снижение количества инцидентов, ускорение реагирования, снижение рисков и соответствие нормативным стандартам.

Приведем примеры показателей эффективности мероприятий в области кибербезопасности. KPI в этом случае могут быть разбиты на 4 группы. Подобное деление поможет не только оценить качество выполняемых работ, но и определить позиции, требующие улучшения, что в свою очередь, позволит быстрее адаптироваться к постоянно меняющимся условиям внешней и внутренней среды для достижения стратегических целей компании.

К первой группе относятся KPI, связанные с ресурсами и процессами, позволяющие оценить выполнение планов и бюджетную эффективность. Это, в первую очередь, такие показатели, как эффективность и своевременное выполнение запланированных мероприятий, процент сотрудников, прошедших обучение и сертификацию и отдача от инвестиций в кибербезопасность.

Ко второй группе относятся KPI, связанные с операционной деятельностью, позволяющие оценить процессную деятельность в области кибербезопасности. Первостепенно нужно понимание процента оперативно устраненных уязвимостей от общего их числа и процента своевременно обработанных заявок пользователей. Отдельно рассматривают показатели, связанные с управлением инцидентами, т.к. они позволяют оценить качество мониторинга ситуации и скорость реагирования на нее. Ключевыми являются пять показателей: среднее время до обнаружения инцидента, среднее время до реагирования на инцидент, количество успешно разрешенных инцидентов, процент завершенных расследований инцидентов, количество повторяющихся инцидентов. Конечно же, необходимо уделить внимание оценке процента нарушений политик безопасности для дальнейшей оценки разработанных процедур.

К третьей группе относятся KPI по улучшению и развитию, позволяющие оценить проектную деятельность в области кибербезопасности. Здесь оценивают полноту и актуальность разработанных политик и процедур кибербезопасности за счет оценки количества документированных, регулярно пересматриваемых и обновляемых политик безопасности, а так же отслеживания внедрения новых технологий, процедур, политик, направленных на повышение уровня кибербезопасности. Отдельно стоит оценивать процент проектов, включающих практики разработки безопасного программного обеспечения (DevSecOps, от сокр. Development, Security, Operations или по-русски разработка, безопасность, операции) и степень автоматизации процессов безопасности в целом. Проведение аудитов и соответствие их стандартам — еще один показатель, про который нельзя забывать — он характеризуется процентом успешно пройденных аудитов и устранением замечаний, если таковые имеются. Итоговым показателем в этой группе является измерение уровня зрелости кибербезопасности, проводимое на постоянной основе (желательно ежегодно).

К четвертой группе относятся KPI, связанные с внутренней и внешней средой, позволяющие оценить процесс обучения, результативность тренировок и качество взаимодействия с партнерами в области

кибербезопасности. Основные показатели, касающиеся анализа результатов обучения и тренировок, заключаются в оценке количества проведенных учебных мероприятий и тренировок по кибербезопасности в год, регулярность и глубина обучения и тренировок, уровень охвата обучением сотрудников. Если говорить о внешнем взаимодействии с поставщиками и партнерами, то следует анализировать процент учета кибербезопасности в корпоративных решениях, количество решений, в которых учитывались риски кибербезопасности, как процент от общего числа решений, а также количество и качество совместных проектов с внешними партнерами по безопасности и эффективность участия в профессиональных сообществах [4].

В мае 2024 года ФСТЭК России была утверждена «Методика оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», в которой внимание сместилось на оценку способности систем оперативно адаптироваться к угрозам и предоставлять доказательства защищенности [4, 5].

Аудит действий администраторов охватывает отслеживание действий администраторов и пользователей с повышенными привилегиями — любая активность должна быть прозрачной, документально фиксированной и с возможностью ее проверить.

В работе с инцидентами важно автоматически фиксировать попытки несанкционированного доступа, формировать их хронологию и анализировать каждый инцидент, т.е. интерпретировать их в режиме реального времени.

Цифровые оказательства предполагает автоматизированную регистрацию нарушения и возможность его хранения в юридически значимом виде.

Аналитика событий — новое веяние, порожденное использованием искусственного интеллекта — возникла необходимость понимания того, что происходит, а это означает: выявлять отклонения в поведении, обнаруживать аномалии и самое главное, строить хронологии атак на основе поведенческих признаков.

Также важно, чтобы охват аудита составлял не менее 80-90% и для оборудования, и для программного обеспечения [5].

Следовательно, в настоящее время, основной акцент сделан на управлении инцидентами, аудите действий администраторов и аналитике.

#### СПИСОК ЛИТЕРАТУРЫ

1. Минцифры оценило прямой ущерб от киберпреступлений в РФ в 160 млрд рублей в год [Электронный ресурс]. URL: <https://tass.ru/ekonomika/23299255> (дата обращения 05.08.2025).
2. Ущерб от киберпреступлений в РФ достиг 120 млрд рублей за семь месяцев [Электронный ресурс]. URL: <https://www.dp.ru/a/2025/08/30/ushherb-ot-kiberprestuplenij> (дата обращения 30.08.2025).
3. 14 показателей кибербезопасности и ключевых показателей эффективности, которые необходимо отслеживать в 2025 году [Электронный ресурс]. URL: <https://www.upguard.com/blog/cybersecurity-metrics#:~:text=Cybersecurity%20success%20is%20measured%20by, and%20compliance%20with%20regulatory%20standards.> (дата обращения 31.08.2025).
4. Ключевые показатели эффективности для подразделений информационной безопасности [Электронный ресурс]. URL: <https://www.itsec.ru/articles/klyuchevye-pokazateli-effektivnosti-dlya-podrazdelenij-informacionnoj-bezopasnosti> (дата обращения 18.08.2025).
5. Какие показатели информационной безопасности особенно важны в 2025 году [Электронный ресурс]. URL: <https://companies.rbc.ru/news/DEVhFZuNuW/kakie-pokazateli-informatsionnoj-bezopasnosti-osobЕННО-vazhnyi-v-2025-godu/?ysclid=mg40zpwjbi282613930> (дата обращения 15.08.2025).

УДК 004.9

#### УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПОСТРОЕНИИ КОРПОРАТИВНОГО ОБЛАЧНОГО АНАЛИТИЧЕСКОГО РЕШЕНИЯ

**Бобчинский Артем Евгеньевич, Андреевский Игорь Леонидович**

Санкт-Петербургский государственный экономический университет,

Садовая ул., 21, Санкт-Петербург, 191023, Россия

e-mails: bobchinskiy.a@unecon.ru, ail@unecon.ru

**Аннотация.** Рассмотрены и систематизированы угрозы информационной безопасности при построении корпоративного аналитического решения. Предложены подходы, связанные с минимизацией рисков информационной безопасности.

**Ключевые слова:** угрозы; информационная безопасность; корпоративное аналитическое решение; анализ данных; визуализация; облачная аналитика.

#### INFORMATION SECURITY THREATS WHEN BUILDING A CORPORATE CLOUD ANALYTICAL SOLUTION

**Bobchinskiy Artem, Andreevskiy Igor**

Saint-Petersburg State University of Economics

21 Sadovaya St, St. Petersburg, 191023, Russia

e-mails: bobchinskiy.a@unecon.ru, ail@unecon.ru

**Abstract.** The threats to information security in the construction of a corporate analytical solution are considered and systematized. Approaches related to the minimization of information security risks are proposed.

**Keywords:** threats; information security; enterprise analytics solution; data analysis; visualization; cloud analytics.

В условиях цифровой трансформации данные становятся важным активом для организаций, позволяя принимать обоснованные решения, совершенствовать бизнес-процессы и разрабатывать новые продукты и услуги.

Рост объемов корпоративных данных привел к формированию новой экономики данных, где их обработка и анализ становятся ключевыми ресурсами и драйверами инновационного развития. В условиях стремительного роста данных, облачные аналитические сервисы стали востребованным инструментом для быстрого и гибкого анализа информации. С учетом текущей ситуации активно начали использоваться как отечественные облачные аналитические сервисы, так и решения на базе программного обеспечения с открытым исходным кодом [6].

Наиболее популярными отечественными и open-source аналитическими системами и BI-платформами являются (в алфавитном порядке) являются: Alpha BI, Loginom, Luxms BI, Metabase, Modus BI, PIX BI [4], PolyAnalyst, Polymatica, Visiology [5], Yandex DataLens [2], Форсайт. Аналитическая платформа и др.

Каждое из представленных на рынке решений имеет ряд своих особенностей в области информационной безопасности [1].

Существующие облачные аналитические решения в большинстве своем предоставляются по модели SaaS (Software as a Service). Для некоторых возможен вариант установки и развертывания в локальном частном облаке с использованием Docker или Kubernetes. Далеко не все из представленных на рынке решений могут импортировать внутрь первичные данные, а работают только через подключение к ним, что требует хранения настроек, логинов и паролей внутри аналитической платформы, что не всегда является подходящим сценарием.

При выборе платформы для построения корпоративного облачного аналитического решения важным моментом остается использование облачных платформ с проверенной репутацией и сертификациями, например, ISO 27001 [3], SOC 2 и др.

Для тех проектов, которые разрабатывались авторами, наиболее существенными ограничениями являлись — необходимость использования частного облака в части накопления и хранения данных, необходимость соблюдения требований по работе с персональными данными (обезличивание данных), возможность предоставления разработанных дашбордов для бизнес-пользователей не только внутри корпоративного контура, но и наружу с использованием механизмов аутентификации и авторизации.

Немаловажным фактором являлась возможность работы команды разработки не только с компьютеров компании, но и дистанционно.

Построение корпоративного аналитического сервиса с использованием облачной аналитической платформы, в особенности если оно ориентировано не только на внутренних пользователей, сопряжено с рядом угроз в области информационной безопасности и имеет ряд своих особенностей.

В общем виде к числу «узких мест» и угроз информационной безопасности можно отнести:

- выбор места размещения первичных данных для анализа (локальное или общественное облако);
- особенности работы с персональными данными;
- использование слабых паролей или недостаточно защищенных учетных записей;
- сложности в обеспечении надежных механизмов аутентификации и авторизации пользователей;
- риск несанкционированного доступа к чувствительной информации, особенно при передаче и хранении данных в облаке;
- угрозы со стороны сотрудников или партнеров, обладающих доступом к платформе;
- возможность утечки данных из-за уязвимостей в инфраструктуре или неправильных настроек;
- отсутствие или слабое шифрование каналов связи;
- ограниченные возможности для мониторинга и аудита действий внутри облачной платформы;
- трудности в отслеживании инцидентов безопасности;
- угрозы при интеграции облачных аналитических платформ с внутренними корпоративными системами и сторонними сервисами и др.

На начальной стадии проекта необходимо определиться не только с целью создания проекта, источниками первичных данных, способами и периодичностью их визуализации, но и со списком заинтересованных сторон и ключевых пользователей создаваемого решения, назначить режим доступа к информационным ресурсам. При этом следует руководствоваться принципами Zero Trust Architecture, при котором ни один пользователь или устройство не считается доверенным без многоуровневой проверки, например, классической двухфакторной аутентификации.

Доступ к первичным данным из нескольких корпоративных информационных систем требует логинов и паролей, что является вопросом доверия от тех специалистов, которые их предоставляют для создаваемого аналитического решения. Так как приходится иметь дело с персональными данными, то все специалисты, вовлеченные в процесс первичной обработки данных обязаны подписать соответствующие документы, в которых прописана ответственность за ненадлежащее использование и разглашение этих данных.

Аналитическая BI платформа в качестве первичной информации может использовать данные из файловой системы или из таблиц баз данных. Если требуется актуальная аналитика в виде различных визуализаций на дашборде, то необходимо настраивать расписания для обновления данных.

Работа с выгруженными данными учетных корпоративных систем в формате файлов MS Excel, текстовых файлов с разделителями (csv) в плане информационной безопасности имеет ряд своих недостатков, так как

требует использования встроенных средств (шифрование файловой системы, настройка прав доступа на общую папку с файлами с первичными данными и пр.

В этом плане работа с первичными данными из таблиц базы данных более предпочтительна, так как изначально требует соответствующих прав доступа как минимум на чтение данных. Также база данных может быть изначально зашифрована встроенными средствами и поддерживать прозрачное шифрование или же размещаться на шифруемом носителе, который шифруется с использованием аппаратных возможностей или средствами операционной системы.

Удаленная разработка дашбордов и доступ к размещенной во внутреннем контуре частного облака облачной аналитической платформе и первичной информации является нетривиальной задачей для администраторов компании, требует нестандартных настроек и постоянных консультаций со специалистами технической поддержки вендора облачной аналитики.

На финальной стадии развертывания и начале промышленной эксплуатации также нельзя забывать об потенциальных дырах в системе информационной безопасности, когда требуется отслеживать злонамеренные действия со стороны недобросовестных пользователей или потенциальных злоумышленников.

К сожалению, опыт использования нескольких программных продуктов говорит о том, что не всегда хватает текущих возможностей логирования всех действий, аудита доступа и мониторинга активностей.

Для минимизации потенциального ущерба от возможных угроз в сфере информационной безопасности при построении корпоративного облачного аналитического решения желательно анонимизировать данные с целью защиты конфиденциальности пользователей и соблюдения законодательства о защите данных [7], размещать их в контролируемом корпоративном облаке, минимизировать поверхность атаки за счет грамотной политики управления пользовательским доступом, контроля сессий и ввода временных ограничений доступа, разграничением доступа к отдельным столбцам и записям наборов первичных данных, контролем за ссылками на опубликованные для общего доступа дашборды и пр.

При построении корпоративного облачного аналитического решения необходимо уделять особое внимание вопросам информационной безопасности. Только системный и проактивный подход позволит минимизировать риски и обеспечить надежную защиту корпоративных данных.

#### СПИСОК ЛИТЕРАТУРЫ

1. Безопасность данных в BI-системе [Электронный ресурс]. URL: <https://habr.com/ru/companies/modusbi/articles/801715> (дата обращения: 30.07.2025).
2. Корпоративная облачная Business Intelligence платформа Yandex DataLens [Электронный ресурс]. <https://datalens.ru/> (дата обращения: 30.07.2025).
3. Официальный сайт для стандартов серии ISO 27001 [Электронный ресурс]. URL: <https://www.iso.org/ru/standard/27001> (дата обращения: 30.07.2025).
4. Российская корпоративная Business Intelligence платформа PIX BI [Электронный ресурс]. URL: <https://pix.ru/products/pix-bi/bi> (дата обращения: 30.07.2025).
5. Российская корпоративная Business Intelligence платформа Visiology [Электронный ресурс]. URL: <https://ru.visiology.ru> (дата обращения: 30.07.2025).
6. Топ 10 лучших BI-систем: сравнение и обзор систем аналитики [Электронный ресурс]. URL: <https://spb.1cbit.ru/blog/top-10-luchshikh-bi-sistem-sravnenie-i-obzor-sistem-analitiki> (дата обращения: 30.07.2025).
7. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ [Электронный ресурс]. URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_61801](https://www.consultant.ru/document/cons_doc_LAW_61801) (дата обращения: 30.07.2025).

УДК 004

#### ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БОЛЬШИХ ДАННЫХ В ЗАДАЧАХ ЭКОНОМИКИ И УПРАВЛЕНИЯ

**Аникин Юрий Викторович, Шилков Владимир Ильич, Ивакина Мария Дмитриевна**

Уральский федеральный университет имени первого Президента России Б.Н. Ельцина,

Мира ул., 19, Екатеринбург, 620062, Россия

e-mails: [anikin-urfu@yandex.ru](mailto:anikin-urfu@yandex.ru), [vi.shilkov@urfu.ru](mailto:vi.shilkov@urfu.ru), [mashaivakina26@gmail.com](mailto:mashaivakina26@gmail.com)

**Аннотация.** Обсуждаются вопросы повышения уровня информационно-экономической безопасности технологии обработки больших данных и метода Data-Driven, предполагающего принятие управленческих решений на основе данных. Большие данные предлагается рассматривать как объект защиты и как средство повышения уровня информационной безопасности.

**Ключевые слова:** информационная безопасность; технология Big Data; метод Data-Driven, «озеро данных».

#### INFORMATION SECURITY OF BIG DATA IN THE TASKS OF ECONOMICS AND MANAGEMENT

**Anikin Yuriy, Shilkov Vladimir, Ivakina Maria**

Ural Federal University named after the First President of Russia B. N. Yeltsin

19 Mira St, Yekaterinburg, 620062, Russia

e-mails: [anikin-urfu@yandex.ru](mailto:anikin-urfu@yandex.ru), [vi.shilkov@urfu.ru](mailto:vi.shilkov@urfu.ru), [mashaivakina26@gmail.com](mailto:mashaivakina26@gmail.com)

**Abstract.** The issues of increasing the level of information and economic security of big data processing technology and the Data-Driven method, which involves making managerial decisions based on data, are discussed. Big data is proposed to be considered as an object of protection and as a means of increasing the level of information security.

**Keywords:** information security; Big Data technology; Data-Driven method; «data lake».

Методы принятия решений, основанные на анализе больших данных, позволяют компаниям адаптироваться к условиям глобальной конкуренции и получать устойчивые стратегические преимущества. Эффективность этих решений, в свою очередь, во многом зависит от методов обработки и анализа структурированной и неструктурированной информации.

Актуальность решения вопросов, связанных с обеспечением информационной безопасности данных обусловлена целым рядом причин, к которым, следует отнести: зависимость конечных результатов анализа от достоверности исходной информации; лавинообразное увеличение объемов и сложности обрабатываемой информации; риски умышленного искажения исходной информации; появление инновационных и эффективных методов обработки данных. Широкое распространения сквозных технологий повлекло за собой увеличение числа инцидентов, связанных с утечкой данных в коммерческих организациях, государственных структурах и органах государственной власти. Автор работы [1], на основании проведенного анализа рисков информационной безопасности, делает вывод, что в Российской Федерации: наблюдается сформированный устойчивый тренд роста количества утечек массивов ценной структурированной и неструктурированной информации, которые в совокупности, влекут за собой утрату миллионов записей персональных данных и приводят к значительным финансовым ущербам, ежегодно достигающим сотни миллионов в долларовом эквиваленте.

Данное обстоятельство не только подтверждает необходимость совершенствования законодательных основ и создания механизмов управления рисками информационной безопасности, но и требует повсеместного внедрения инновационных технических инструментов защиты информации. В соответствии с [2], для обеспечения необходимого уровня информационной безопасности больших данных необходимо не только вложение значительных финансовых средств, но и применение системного подхода, предполагающего сочетание тактических и стратегических решений при: внедрении передовых принципов повышения конфиденциальности в процессах управления данными; внесении изменений и дополнений в правила защиты персональных данных; организации многоаспектного мониторинга; шифровании и разделении больших данных; управлении авторизацией и идентификацией в процессе контроля доступа.

В соответствии с [3] с помощью анализа больших данных, осуществляемого в целях повышения уровня информационной безопасности возможно: повысить эффективность противодействия деструктивным воздействиям посредством автоматизации рутинных процедур и эффективного анализа рисков, основанного на данных; организовать проактивное предотвращение угроз путем выявления и устранения уязвимостей до того, как ими воспользуются злоумышленниками; ускорить расследование инцидентов и принятие мер по смягчению последствий; повысить скорость и точность обнаружения кибератак и других угроз безопасности. Так, например, за счет более глубокой аналитики, применение технологии Big Data для борьбы с мошенническими схемами может оказать положительное влияние на состояние информационно-экономической безопасности компонентов финансово-кредитной и банковской системы. Информационная безопасность и борьба с мошенничеством обеспечивается, в числе других мероприятий, с помощью алгоритмов обработки информации.

Технологии Big Data позволяют отслеживать аномалии в транзакциях и распознавать шаблоны мошеннических схем. Могут быть решены задачи необходимые для противодействия мошенническим схемам, в том числе задачи контроля и минимизации рисков, классификации клиентов по уровню платежеспособности, выбора оптимальных инновационных методов оценки (поведенческий анализ), разработки методики комплексного подхода к организации риск-менеджмента. Для минимизации кредитных рисков, практически мгновенной проверки кредитной истории клиента и разработки эффективных прогнозов платежеспособности, на основе анализа больших данных могут быть разработаны системы оценки кредитоспособности клиентов, которые могут формировать в автоматическом режиме необходимые документы для выдачи кредитов. Для реализации этой модели финансовая организация интегрирует свою банковскую инфраструктуру по принципу Banking-as-a-Service (BaaS), обеспечивая обмен информацией о клиентах с партнерским банком. При этом фактическое принятие решений по выдаче кредитов и проведение скоринга происходит непосредственно банком, однако все операции выполняются от имени бизнес-партнера.

Вместе с тем, следует отметить, что: зависимости качества аналитики от рисков ошибок в исходной информации и качества входных данных, неточности в которых, в большинстве случаев, не могут быть выявлены и устранены с помощью автоматизированных технологий, так как неполные, устаревшие или содержащие ошибки данные могут привести не только к снижению точности и искажению результатов, но и к неверным прогнозам и неверным управленческим решениям; риски, связанные с конфиденциальностью данных, в том числе риски утечек персональных данных клиентов и другой финансовой конфиденциальной информации, которые могут привести к возникновению угроз для информационной безопасности не только отдельного клиента, проекта, но и всей компании. По мнению авторов работы [4], перспективным направлением развития Big Data является концепция создания централизованного хранилища в виде Security Data Lake (SDL), которое представляет собой единое место для хранения, анализа, сбора данных из множества источников, поиска и использования данных, имеющих отношение к информационной безопасности организации. «Озеро данных»

является развитием технологии SIEM (Security information and event management), предназначено для обслуживания и управления всеми журналами или другими источниками данных и, предоставляет значительные преимущества для хранения и обработки больших данных. Однако, несмотря на то, что многие решения SIEM активно интегрируются с SDL, SIEM применяется преимущественно для анализа ограниченного набора журналов с целью предоставления значимых предупреждений безопасности, а SDL позволяет организовать эффективное выявление и подробное изучение этих угроз, а также реализовать возможности применения алгоритмов искусственного интеллекта и машинного обучения, достигаемое за счет возможности длительного хранения большого объема данных различных типов. Термин «информационная безопасность» в контексте понятия «большие данные», возможно обсуждать в нескольких различных аспектах. Так, например, если большие данные рассматривать в качестве объекта, требующего информационной защиты, то должны быть исследованы вопросы повышения уровня информационной безопасности собственно больших данных в процессах сбора, подготовки, передачи и хранения, значительных объемов данных, оценки достоверности собираемой информации и оценки рисков ее искажения, с целью последующего использования этих данных для конкретных целей, в конкретных сферах, и для решения конкретных задач. В другом аспекте, могут быть исследованы вопросы возможности применения больших данных для разработки эффективных инструментальных средств защиты информации в различных социально-экономических задачах. К этим вопросам могут быть отнесены вопросы, связанные как с положительным влиянием применения результатов технологии Big Data на уровни информационной безопасности конкретных объектов, процессов и задач, так и с рисками применения некорректной аналитики и неверных выводов, сделанных на основе обработки массивов больших данных. В этом случае, можно считать, что технология Big Data выступает инструментальным средством, с помощью которого будут созданы эффективные средства защиты информации.

Таким образом, появление технологий обработки и анализа больших данных привело к возникновению новых возможностей для разработки эффективных инструментальных средств для повышения безопасности защищаемых объектов. К основным проблемам, препятствующим созданию эффективных систем информационной безопасности относится необходимость: поиска, фильтрации и анализа большого объема неструктурированных данных; разработки новых технологических подходов к сбору, обработке, анализу больших объемов информации; привлечения квалифицированных экспертов в области информационной безопасности; разработки новых стратегий информационной безопасности, адаптированных к архитектурам Big Data на основе комплексного подхода. Успешное внедрение метода управления, основанного на анализе данных (Data-Driven) и технологии обработки и анализа данных Big Data в теорию и практику управления сложными социально-экономическими системами требует решение целого ряда организационно-технологических проблем, часть из которых связана с вопросами информационной безопасности больших данных.

#### СПИСОК ЛИТЕРАТУРЫ

1. Яхтин В.А. Национальные информационные риски больших данных // Вестник Волгоградского государственного университета. Экономика. 2021. Т. 23. № 3. С. 16-25.
2. Артюшкин О.В., Рачинская М.А. Систематизация проблем больших данных и вариантов их решения // Инженерные технологии: традиции, инновации, векторы развития. Материалы X Всероссийской научно-практической конференции с международным участием. Абакан, 2024. С. 9-11.
3. Савва Ю.Б., Савва Т.Ю. Аналитика больших данных и задачи обеспечения информационной безопасности // Цифровой регион: опыт, компетенции, проекты. Сборник статей VI Международной научно-практической конференции, посвященной 25-летию Юбилею инженерно-экономического института, проводимой в рамках Десятилетия науки и технологий в России. Брянск, 2024. С. 651-655.
4. Секерко А.А., Чесалин А.Н. Современные проблемы анализа и хранения больших данных в информационной безопасности // Прикладные процессы в области информационной безопасности. Тенденции развития методов защиты информации. Материалы научно-практических конференций. Самара, 2023. С. 56-58.

УДК 004

#### ЦИФРОВАЯ ТРАНСФОРМАЦИЯ СИСТЕМ ВОДОСНАБЖЕНИЯ И КИБЕРБЕЗОПАСНОСТЬ

**Аникин Юрий Викторович, Шилков Владимир Ильич**

Уральский федеральный университет имени первого Президента России Б.Н. Ельцина

Мира ул., 19, Екатеринбург, 620062, Россия

e-mails: anikin-urfu@yandex.ru; vi.shilkov@urfu.ru

**Аннотация.** Обсуждаются технологические, организационные особенности и проблемы цифровой трансформации систем водоснабжения в Российской Федерации и за рубежом. Показаны перспективные направления цифровизации водоканалов, отмечены причины отставания отечественных водоканалов. Обозначены риски и киберугрозы для безопасности предприятий водного сектора.

**Ключевые слова:** цифровая трансформация; системы водоснабжения; риски; кибербезопасность.

#### DIGITAL TRANSFORMATION OF WATER SUPPLY SYSTEMS AND CYBERSECURITY

**Anikin Yury, Shilkov Vladimir**

Ural Federal University named after the First President of Russia B.N. Yeltsin

19 Mira St., Yekaterinburg, 620062, Russia

e-mails: anikin-urfu@yandex.ru; vi.shilkov@urfu.ru

**Abstract.** Technological, organizational features and problems of digital transformation of water supply systems in the Russian Federation and abroad are discussed. Promising directions of digitalization of water utilities are shown, the reasons for the lag of domestic water utilities are noted. The risks and cyber threats to the security of water sector enterprises are outlined.

**Keywords:** digital transformation; water supply systems; risks; information security.

Одним из важных приоритетов для устойчивого развития и надежного существования урбанизированных территорий во всем мире является бесперебойная работа и безопасное управление их системами водоснабжения. Наличие качественной питьевой и технической воды для населения и промышленности, получение ее в необходимом количестве становится, наряду с другими составляющими, основой для прогресса экономики и социального развития общества, обеспечения высокого качества жизни людей.

В последние несколько десятилетий потребление воды для хозяйственно-бытовых и производственных нужд в городах значительно выросло. Это связано как с ростом населения городов, так и с развитием в них высоко технологичных отраслей промышленности, требующих увеличенных расходов воды, надежности и бесперебойности ее подачи к объектам потребления. При этом многие города испытывают острую нехватку воды в тех близко расположенных поверхностных или подземных источниках, которые они использовали в течение длительного времени. Такая ситуация вынуждает искать другие приемлемые источники, которыми часто становятся поверхностные источники, обладающие необходимыми расходами. Однако часто их использование требует значительных финансовых и материальных затрат уже на стадии освоения. Эти затраты связаны с транспортировкой воды на большие расстояния, ее очисткой до нормативных показателей, строительством необходимой водной инфраструктуры, защитой источников от загрязнения [1].

Анализируя работу систем водоснабжения, можно отметить, что различные недостатки в работе этих систем отрицательно сказываются как на жизни населения, так и на стабильной работе других инфраструктурных городских объектов: промышленность, энергетика, транспорт.

Специфика развития водопроводных систем в разных регионах и городах обусловлена определенными различиями в условиях их формирования, во времени начала сооружения сетей и объектов, техническом уровне. Конечно, состав водопроводных систем и уровень их развития могут существенно различаться, что сказывается на социальном и экономическом развитии городов. Тем не менее проблемы водоснабжения многих крупных городов, в первую очередь с большой историей во многом схожи. Это старение таких систем (увеличенное число аварий, физический и моральный износ сетей и сооружений, недостаточная эффективность). На эти причины могут наслаиваться и другие факторы: изменчивость гидрологического режима источника, нехватка и недостаточная квалификация персонала, чрезвычайные ситуации природного и антропогенного характера. Обновление стареющей водной инфраструктуры городов часто отстаёт от растущих потребностей в воде, поэтому вопросы функционирования городских систем водоснабжения и внедрения новых технологий (цифровизация, искусственный интеллект) с учетом их безопасности являются актуальными и широко освещаются в отечественной и зарубежной научной прессе [2-5].

Цифровизация открывает перед водной отраслью новые перспективы, которые связаны с обработкой и анализом больших данных, автоматизацией бизнес-процессов, корректировкой технологических процессов в режиме реального времени, прогнозированием и минимизацией рисков. Они могут помочь водоканалам в решении вопросов продления срока службы оборудования, сокращения утечек и аварийности на водопроводной сети, содействия сохранению и рациональному распределению водных ресурсов. Реальная заслуга цифровизации состоит в том, что она позволяет использовать интеллектуальное усиление для интерпретации структурированных и всё более неструктурированных данных, основанных на текстовых данных или показаниях датчиков. Когнитивный анализ повысит эффективность извлечения пользы из этих данных, а также выполнения или автоматизации последующих оптимальных действий на основе анализа прогнозных и предписывающих данных.

Сообщается [6], что в Российской Федерации «на сегодняшний день (апрель 2023 г.) предприятия водоснабжения и водоотведения в год суммарно тратят 5-6 млрд руб. на ИТ и цифровые проекты. Прогноз аналитиков РИР (АО «Русатом Инфраструктурные решения») говорит о том, что к 2030 году при сохранении текущих темпов развития рынка затраты на такие проекты могут вырасти до 8-9 млрд руб.».

В отчете компании Research and Markets [7] показано, что мировой «Рынок цифровых решений делится на 6 сегментов:

- интеллектуальный учет воды;
- интеллектуальные онлайн-датчики воды;
- интеллектуальные решения для обнаружения утечек и управления NRW;
- решения для интеллектуального управления и оптимизации трубопроводных сетей (включая интеллектуальные насосы и насосные станции);
- цифровые решения-близнецы;
- интеллектуальное управление и обслуживание (включая управление активами предприятия и мониторинг состояния активов)».

В отчете также было выявлено 30 различных способов применения цифровых решений в сфере водоснабжения и представлены 20 ведущих цифровых акселераторов, которые в настоящее время предлагают передовые цифровые решения для предприятий водоснабжения.



Следует отметить, что реализация стратегии цифровизации и ее внедрение в технологические процессы в большинстве отечественных водоканалов отстают от передовых зарубежных водоканалов и происходят с определённой задержкой по ряду причин, к которым можно отнести:

- нехватку финансовых средств;
- нехватку или даже отсутствие в структуре водоканалов ИТ-специалистов;
- отсутствие современного программного обеспечения для осуществления цифровизации;
- старение рабочей силы и недостаточное количество квалифицированных специалистов технического профиля;
- несовершенство нормативно-правового регулирования.

Процесс цифровой трансформации влечет за собой все более тесную интеграцию между физическим и кибернетическим уровнями системы водоснабжения. Эта интеграция повышает эффективность и улучшает мониторинг, но в то же время подвергает системы водоснабжения новым угрозам, в том числе кибератакам. Большинство предприятий отрасли по ряду причин не способны противостоять комбинированным кибератакам, что вызывает серьёзную озабоченность [8]. В водном секторе отсутствует коллективная ситуационная осведомлённость о киберугрозах. Организациям важно уделять приоритетное внимание кибербезопасности и принимать разумные меры для предотвращения, обнаружения и реагирования на киберинциденты.

Таким образом, на основании проведенного исследования можно сделать вывод, что в современных условиях цифровая трансформация водной отрасли стала ключевым решением для достижения стоящих перед ней целей. Цифровые решения способны значительно повысить эффективность и оптимизировать всю водную инфраструктуру, связанную с различными сферами человеческой деятельности. Однако безопасность систем водоснабжения подвергается серьезным угрозам, что вызывает все большую обеспокоенность и требует принятия неотложных мер.

#### СПИСОК ЛИТЕРАТУРЫ

1. Figueiredo I., Esteves P., Cabrita P. Water wise — a digital water solution for smart cities and water management entities *Procedia Computer Science* 181 2021, P. 897–904 URL: [https://www.sciencedirect.com/science/article/pii/S187705092100288X?ref=pdf\\_download&fr=RR-2&pt=9722d1dc8b263f0f](https://www.sciencedirect.com/science/article/pii/S187705092100288X?ref=pdf_download&fr=RR-2&pt=9722d1dc8b263f0f) (Дата обращения: 20.08.2025).
2. C. Bosco, G.S. Raspati, K. Tefera at al. Protection of Water Distribution Networks against Cyber and Physical Threats: The STOP-IT Approach Demonstrated in a Case Study *Water* 14(23):3895 URL: [https://www.researchgate.net/publication/365875510\\_Protection\\_of\\_Water\\_Distribution\\_Networks\\_against\\_Cyber\\_and\\_Physical\\_Threats\\_The\\_STOP-IT\\_Approach\\_Demonstrated\\_in\\_a\\_Case\\_Study](https://www.researchgate.net/publication/365875510_Protection_of_Water_Distribution_Networks_against_Cyber_and_Physical_Threats_The_STOP-IT_Approach_Demonstrated_in_a_Case_Study) (Дата обращения: 20.08.2025).
3. D. Nikolopoulos, G. Moraitis, C. Makropoulos Strategic and Tactical Cyber-Physical Security for Critical Water Infrastructures In book: *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: Securing Critical Infrastructures in Air Transport, Water, Gas, Healthcare, Finance and Industry* (2021) [https://www.researchgate.net/publication/354606538\\_7\\_Strategic\\_and\\_Tactical\\_Cyber-Physical\\_Security\\_for\\_Critical\\_Water\\_Infrastructures](https://www.researchgate.net/publication/354606538_7_Strategic_and_Tactical_Cyber-Physical_Security_for_Critical_Water_Infrastructures) (Дата обращения: 20.08.2025).
4. A. M. Omotayo Cybersecurity and water utilities: factors for influencing effective cybersecurity implementation in water sector (2021) Conference: *Proceedings of the American Society for Engineering Management 2020 International Annual Conference* H. Keathley, J. Enos and M. Parrish eds. At: United States Conference URL: <https://www.researchgate.net/publication/365875510> (Дата обращения: 20.08.2025).
5. Enabling digital transformation in smart sustainable cities—master plan. UNEP, UNDESA, UNU and ITU 2023. URL: [https://www.itu.int/en/publications/Documents/tsb/2023-Master-plan-Enabling-digital-transformation-smart-cities/files/downloads/23-00351\\_Master-plan-Enabling-digital-transformation-smart-cities.pdf](https://www.itu.int/en/publications/Documents/tsb/2023-Master-plan-Enabling-digital-transformation-smart-cities/files/downloads/23-00351_Master-plan-Enabling-digital-transformation-smart-cities.pdf) (Дата обращения: 20.08.2025).
6. В «Русатом Инфраструктурные решения» оценили потенциал цифровизации предприятий водоснабжения URL: <https://www.rusatom-utilities.ru/media-center/news/v-rusatom-infrastrukturnye-resheniya-otsenili-potentsial-tsifrovizatsii-predpriyatii-vodosnabzheniya/> (Дата обращения: 20.08.2025).
7. Digital Water Solutions and Services Growth Opportunities. Report. Frost & Sullivan. 2022. 82 p. URL: [https://www.researchandmarkets.com/reports/5558086/digital-water-solutions-and-services-growth?utm\\_source=GNOM&utm\\_medium=PressRelease&utm\\_code=5qp2hf&utm\\_campaign=1676356+-+Top+5+Predictions+for+Digital+Water+Solutions+and+Services+Market+2022&utm\\_exec=cari18prd](https://www.researchandmarkets.com/reports/5558086/digital-water-solutions-and-services-growth?utm_source=GNOM&utm_medium=PressRelease&utm_code=5qp2hf&utm_campaign=1676356+-+Top+5+Predictions+for+Digital+Water+Solutions+and+Services+Market+2022&utm_exec=cari18prd) (Дата обращения: 20.08.2025).
8. Germano J. H. Cybersecurity Risk & Responsibility in the Water Sector. American Water Works Association URL: <https://awwa.org/Portals/0/AWWA/Government/AWWACybersecurityRiskandResponsibility.pdf?ver=2018-12-05-123319-013>. (дата обращения: 20.08.2025).

УДК 004.9

#### ОТ ИНВЕНТАРИЗАЦИИ ДО ЗАЩИТЫ ИНФОРМАЦИИ: ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ ПРАКТИКИ УПРАВЛЕНИЯ ИТ-АКТИВАМИ В КОНТУРЕ ИНФОРМАЦИОННО БЕЗОПАСНОСТИ

Василисин Павел Сергеевич

Санкт-Петербургский государственный экономический университет,

Садовая ул., 21, Санкт-Петербург, 191023, Россия

e-mail: vasilisin.ps@gmail.com

**Аннотация.** Предлагаются подходы, позволяющие применять практики управления ИТ-активами в целях обеспечения защиты информации организации.

**Ключевые слова:** управление; ИТ-активы; инструмент контроля; инвентаризация; информационная безопасность.

**FROM INVENTORY TO CYBER-PROTECTION: PRACTICAL APPLICATION OF IT-ASSET MANAGEMENT PRACTICES IN THE INFORMATION SECURITY CONTEXT****Vasilisin Pavel**

St. Petersburg State University of Economics  
21 Sadovaya St, St. Petersburg, 191023, Russia  
e-mails: vasilisin.ps@gmail.com

**Abstract.** The article proposes practices that allow for the use of IT-asset management practices to ensure the protection of an organization's information.

**Keywords:** control; IT-assets management; control tools; inventory; information security.

Практика работы за последние месяцы показала, что даже крупные рыночные игроки несут существенные риски компрометации информации, утечки данных, а также риски доступа на их сервера и контейнеры хакерских программ.

Как известно, управление любым объектом строится на полном понимании всех составных частей и структуры данного объекта, будь это набор данных, или целый ЦОД с множеством физических и виртуальных машин, СХД и базами данных. При наличии структурированной информации о размещении объектов физической и программной инфраструктуры обеспечивается возможность всестороннего анализа для исключения рисков информационной безопасности.

Достоверные данные для проведения данного анализа могут поставляться со стороны службы управления ИТ-активами. Функциональное направление «ИТ-активы» обладает не только данными бухгалтерского учета, но и так называемыми данными оперативного учёта, уточняющими дополнительные атрибуты, необходимые ИБ.

Главный враг информационной безопасности при анализе данных об ИТ-инфраструктуре — так называемые «shadow IT» (теневые ИТ, или «слепые зоны») [1-3].

Функциональное направление «ИТ-активы» способно исполнять задачи автоматизированного обнаружения и учёта. Реализация данной задачи требуется не только для обеспечения учёта или контроля инвестиционного процесса, но может быть применено для выявления программной и аппаратной ИТ-инфраструктуры, возникающей в периметре организации без требуемого согласования.

Вторая важная задача, решаемая ИТ-активами, которая может быть использована со стороны ИБ-анализ на базе категоризации и атрибутирования. ИТ-активы собирают информацию об операционных системах, прикладном ПО, версиях ПО, владельцах и объеме инсталляций, категориях критичности актива для бизнеса, статусе обновления, серийном номере, площадке и пр. Все эти данные могут помочь мгновенно принять решение о работе с объектом ИТ-инфраструктуры.

Следующая возможная задача-интеграция с системами защиты. Притом интеграция может быть двухсторонней. Не только данные, поступающие со стороны ИТ-активов, могут быть использованы для средств защиты информации, но и такие инструменты, как Kaspersky могут быть успешно использованы для получения инвентарных и др. данных об ИТ-активах для принятия управленческих решений, направленных на инвестиционную деятельность в сфере ИТ.

Процессы управления жизненным циклом ИТ-актива могут быть тесно интегрированы с функцией информационной безопасности. Например, при вводе объекта в эксплуатацию может реализовываться автоматическое применение базового уровня защиты. При эксплуатации может быть реализован регулярный контроль критичности и пересчёт, а также сканирование уязвимости. При выводе из эксплуатации обеспечивается гарантированное удаление данных с носителей, исключение из всех учетных систем [4-7].

Таким образом, построение эффективного контура информационной безопасности — это не столько вопрос выбора и внедрения самых дорогих инструментов защиты, сколько задача создания прочного фундамента из точных и актуальных данных. Как мы убедились, этим фундаментом является система комплексного и автоматизированного управления ИТ-активами. Безопасность без полного понимания что именно нужно защищать — неэффективна и ресурсоемка. Она подобна попыткам охранять невидимого противника в темной комнате. Такие процессы как «Обнаружение», «Категоризация», «Интеграция» и «Управление жизненным циклом» представляют собой не разрозненные действия, а единый непрерывный цикл. Именно этот цикл позволяет трансформировать статичный список «железа и софта» в динамическую систему контекстной безопасности.

Внедрение культуры глубокого понимания и управления своими ИТ-активами — это не технический нюанс, а стратегическая необходимость. Это тот самый мост, который соединяет технические возможности инструментов защиты с реальными бизнес-процессами и экономическими целями компании. Начинать строить свою оборону стоит не с крепостных стен, а с точной карты собственной территории. Только так можно быть уверенным, что каждый ресурс, вложенный в безопасность, работает на максимальный результат.

**СПИСОК ЛИТЕРАТУРЫ**

1. Cartlidge A., Chakravarthy J., Rudd C., Sowerby J.A. Operational Support and Analysis ITIL Intermediate Capability Handbook. London, TSO, 2013. 179 с.
2. Национальный стандарт Российской Федерации ГОСТ ИСО/МЭК 19770/1- Управление ИТ-активами ч.1. Системы управления ИТ-активами. Требования. Москва, 2025.
3. ITIL 4 (IT Infrastructure Library). Practice: Service Configuration Management.
4. NIST Cybersecurity Framework (CSF) 2.0.
5. Gartner. IT Asset Management (ITAM) and How to Build an Effective ITAM Program.
6. Harris, S., Maymi, F. CISSP All-in-One Exam Guide.
7. Постановление Правительства Российской Федерации от 01.07.2024 г. О порядке учета ИТ-активов, используемых для осуществления деятельности по цифровой трансформации системы государственного (муниципального) управления.

УДК 621.391

## КОРПОРАТИВНЫЙ ПОДХОД К ОРГАНИЗАЦИИ МНОЖЕСТВЕННОГО ДОСТУПА К ИНФОКОММУНИКАЦИОННЫМ РЕСУРСАМ

Верзун Наталья Аркадьевна<sup>1</sup>, Колбанёв Михаил Олегович<sup>1</sup>, Кунтуров Андрей Леонидович<sup>2</sup>

<sup>1</sup> Санкт-Петербургский государственный экономический университет

Канала Грибоедова наб., 30-32, лит. А, Санкт-Петербург, 191023, Россия

<sup>2</sup> Санкт-Петербургский государственный университет аэрокосмического приборостроения

Большая Морская ул., 67, Санкт-Петербург, 190000, Россия

e-mails: verzun.n@unecon.ru, mokolbanev@mail.ru, kunturov@rambler.ru

**Аннотация.** Рассматривается «корпоративный» подход к организации доступа к сетевым ресурсам. «Корпоративность» проявляется в использовании принципа «справедливого распределения» общего ресурса, в частности, канала передачи между участниками информационного взаимодействия. Главное требование к функционированию корпоративной системы множественного доступа — удовлетворение общему критерию оптимальности, в качестве которого предлагается использовать средневзвешенную долю принятых безошибочно и вовремя блоков данных. Предложена математическая модель сети корпоративного множественного доступа, методы расчета вероятностно-временных характеристик передачи блоков данных. Сформулирована задача оптимального распределения канального ресурса и описаны этапы её решения.

**Ключевые слова:** инфокоммуникационные ресурсы; система доступа; корпоративный множественный доступ; критерий оптимальности.

## CORPORATE APPROACH TO THE ORGANIZATION OF MULTIPLE ACCESS TO INFORMATION AND COMMUNICATION RESOURCES

Verzun Natalia<sup>1</sup>, Kolbanev Mikhail<sup>1</sup>, Konturov Andrey<sup>2</sup>

<sup>1</sup> St. Petersburg State University of Economics

30-32 Griboedov Channel Emb, St. Petersburg, 191023, Russia

<sup>2</sup> Saint Petersburg State University of Aerospace Instrumentation

67 Bolshaya Morskaya St, St. Petersburg, 190000, Russia

e-mails: verzun.n@unecon.ru, mokolbanev@mail.ru, kunturov@rambler.ru

**Abstract.** The “corporate” approach to the organization of access to network resources is considered. “Corporatism” is manifested in the use of the principle of “fair distribution” of a common resource, in particular, a transmission channel between participants in information interaction. The main requirement for the functioning of a corporate multiple access system is to meet the general criterion of optimality, which is proposed to use the weighted average proportion of data blocks received accurately and on time. A mathematical model of a corporate multiple access network and methods for calculating the probability-time characteristics of data block transmission are proposed. The problem of optimal channel resource allocation is formulated and the stages of its solution are described.

**Keywords:** information and communication resources; access system; corporate multiple access; optimality criterion.

Необходимость создания нового подхода к организации доступа к информационно-коммуникационным ресурсам обусловлена эволюцией требований к ним. Такие факторы как: возрастающие объемы передаваемых данных, рост числа подключенных устройств, в том числе, умных вещей, увеличение количества мобильных терминалов, широкий спектр вариантов доступа к глобальным информационным ресурсам через эфирные сети и др. стимулируют развитие систем доступа.

Представлена концепция корпоративного алгоритма множественного доступа, где отказываются от идеи конкуренции между источниками нагрузки при разделе общей среды передачи [1]. В данном подходе «корпоративность» предусматривает справедливое распределение канала передачи, обеспечивающее одновременную и своевременную передачу данных от всех источников нагрузки. Оценку качества функционирования системы с корпоративным доступом можно осуществлять с применением общего критерия оптимальности, в качестве которого предлагается использовать, например, средневзвешенную долю принятых безошибочно и вовремя блоков данных, или средневзвешенное среднее время задержки передачи блоков данных, или средневзвешенную долю потерянных блоков данных.

В качестве примера реализации предложенного подхода рассмотрен корпоративный алгоритм множественного доступа на основе комбинированного метода разделения канала передачи: между кластерами источников нагрузки используется временное разделение [2], а внутри каждого кластера — случайный синхронный доступ. Разработаны математическая модель сети корпоративного множественного доступа и метод расчета вероятностно-временных характеристик процесса передачи блоков данных в сети [3]. Сформулирована задача оптимизации: выбор оптимального режима работы сети доступа, который предполагает такое распределение временных окон между кластерами источников нагрузки, при котором достигается экстремум общего критерия оптимальности. Предложен трехэтапный алгоритм решения задачи оптимизации: 1 — расчет всех возможных значений выбранного критерия оптимальности, 2 — построение графической модели задачи оптимизации и 3 — поиск для построенного графа кратчайшего пути. Совокупность ребер, составляющих

кратчайший путь и будет решением оптимизационной задачи. Проведена апробация алгоритма. Выполненные расчеты демонстрируют эффективность применения созданных алгоритмов, моделей и методик.

#### СПИСОК ЛИТЕРАТУРЫ

1. Верзун Н. А. Колбанёв М.О., Советов Б.Я. Корпоративный алгоритм множественного доступа в киберпространстве // Труды учебных заведений связи. 2025. Т. 11, № 3. С. 97-107.
2. Гезалов Э.Б. Модель неоднородной локальной сети связи с протоколом синхронного временного доступа с учетом надежности её элементов. / T-Comm. Телекоммуникации и Транспорт. 2021. Т.15. №3. С.25-29.
3. Вишневский В.М. Теоретические основы проектирования компьютерных сетей. М.: Техносфера. 2003. 512 с.

УДК 004.9

### НЕКОТОРЫЕ АСПЕКТЫ ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ТЕХНОЛОГИЙ ТЕРМИНАЛЬНОГО ДОСТУПА

**Емельянов Александр Александрович, Пескова Елизавета Владимировна**

Санкт-Петербургский государственный экономический университет

Садовая ул., 21, Санкт-Петербург, 191023, Россия

e-mails: S1\_Alex2000@mail.ru, olnicka@mail.ru

**Аннотация.** Рассмотрены основные особенности применения технологий терминального доступа, их проблемные сферы и уязвимости. Описаны существующие средства защиты, выявлены недостатки, предложено новое решение, повышающее степень безопасности терминальной инфраструктуры.

**Ключевые слова:** терминальный доступ; безопасность; RDP уязвимости; несанкционированный доступ; облачные сервисы.

### SOME ASPECTS OF INFORMATION AND ECONOMIC SECURITY IN TERMINAL ACCESS TECHNOLOGIES

**Emelyanov Alexandr, Peskova Elizaveta**

St. Petersburg State University of Economics

21 Sadovaya St, St. Petersburg, 191023, Russia

e-mails: S1\_Alex2000@mail.ru, olnicka@mail.ru

**Abstract.** The main features of the application of terminal access technologies, their problem areas and vulnerabilities are considered. The existing means of protection are described, shortcomings are identified. New solution that increases the security level of the terminal infrastructure is proposed.

**Keywords:** terminal access; security; RDP vulnerabilities; unauthorized access; cloud services.

Технологии терминального доступа позволяют реализовывать централизованное управление вычислительными ресурсами и упрощают работу сотрудников с приложениями без необходимости их локальной установки на пользовательские компьютеры. В рамках облачных моделей обслуживания данный подход имеет название DaaS (Desktop-as-a-Service). С точки зрения реализации бизнес-процессов предприятия использование такой модели обслуживания существенно снижает расходы: как капитальные, сокращающиеся за счёт уменьшения трат на закупку программного и аппаратного обеспечения; так и регулярные, вследствие отсутствия необходимости поддерживать большой парк вычислительной техники и продлять лицензии [1]. Кроме того, упрощение администрирования, возможность оперативного распределения вычислительных ресурсов снижает затраты на оплату работы большого количества профильных сотрудников (системных и сетевых администраторов, devops-специалистов и т.д.)

Описываемая технология имеет весьма существенные уязвимости, связанные с семейством протоколов, входящих в стек RDP, применяемый в качестве стандартного метода взаимодействия клиент-серверной архитектуры в системах терминального доступа. Основным способом получения несанкционированного доступа (НСД) к инфраструктуре предприятия является метод силового, словарного и гибридного перебора паролей (часто называемого в специализированной литературе единым термином brute-force). Применение слабых/однотипных комбинаций, отсутствие многофакторной аутентификации создают значимый риск компрометации критически важных ресурсов компаний, и, вследствие этого — существенные финансово-экономические потери. В первом полугодии 2025 года при возникновении инцидентов, связанных с НСД, уязвимости RDP использовались в 95% случаев от общего числа зафиксированных случаев, что является значительным увеличением по сравнению с 88% в 2024 и 75% в 2023 году. Можно наблюдать тенденцию к существенному возрастанию количества использования специфических особенностей протокола RDP, что подчёркивает необходимость разработки и внедрения комплексных методов защиты в программно-аппаратную инфраструктуру предприятий [2]. На текущий момент в качестве средств защиты обычно используются инструменты мониторинга и блокировки исходных сетевых источников RDP Guard и IPBan в случае наличия нескольких неудачных попыток аутентификации.

Программный комплекс RDP Guard анализирует события, фиксируемые в подсистеме Windows Event Log. При обнаружении нескольких неудачных попыток входа подряд осуществляется блокировка IP-адреса потенциально опасного источника на определённое время. Эта мера эффективно снижает вероятность

компрометации слабых паролей и ограничивает возможность массового перебора, но при этом имеются и существенные ограничения. Механизм блокировки базируется на неудачных попытках входа, что делает его уязвимым к распределённым атакам с использованием множества IP-адресов (так называемые botnet-системы). При этом слишком жёсткие ограничения могут привести к ложным срабатываниям и некорректному ограничению доступа пользователей к терминальной системе предприятия [3].

Метод работы IPVan во многом схож с предыдущим программным решением. Отслеживаются события безопасности, и при выявлении множественных неудачных попыток аутентификации источник трафика автоматически помещается в правила блокировки брандмауэра операционной системы. Однако при этом имеются существенные ограничения в аналитике угроз и корреляции событий, предоставляя лишь блокировку источников трафика.

Более надёжным средством является активное внедрение методов многофакторной аутентификации (MFA). Данный подход усиливает защиту служб удалённых рабочих столов за счёт подтверждения личности с использованием нескольких независимых источников верификации личности. К сожалению, внедрение MFA является весьма дорогостоящим вариантом, особенно для малых организаций. В основном это связано с необходимостью для пользователей применять ряд дополнительных мер защиты, что существенно осложняет их работу и вызывает проблемы функционирования многих бизнес-процессов организаций [4].

С точки зрения авторов, в качестве альтернативного решения может быть применён подход на базе протокола SDP (Session Description Protocol), основанный на модели безопасности с нулевым доверием. Это решение полностью скрывает внутреннюю инфраструктуру до момента успешной аутентификации и авторизации; это значительно снижает вероятность успешного силового перебора с последующим НСД. Ключевой особенностью SDP является создание динамического и строго персонализированного периметра доступа, где каждому присваивается индивидуальный набор прав. Попытки несанкционированного доступа пресекаются на этапе аутентификации с применением некорректных данных.

В рассматриваемом подходе используются динамические модели управления доступом, при которых уровень предоставляемых ресурсов и пропускная способность регулируются с учётом критичности задач и экономической значимости пользователя. Внедрение адаптивной аутентификации на основе анализа стоимости потенциального ущерба позволяет применять усиленные меры контроля для сессий с высокой степенью значимости, одновременно контролируя доступ к менее критичным ресурсам. Распределённые политики доступа, формируемые с учётом совокупной стоимости владения инфраструктурой, обеспечивают рациональное распределение ресурсов терминального доступа и снижение экономических потерь при перегрузках или случаях НСД.

Для построения доверенных зон в SDP используются принципы микроэкономики, учитывающие не только техническую идентичность субъекта, но и его значимость для внутренних бизнес-процессов предприятия. Дополнительно может быть реализована интеграция с системами прогнозирования атак, что обеспечивает предварительное выявление и изоляцию потенциальных векторов угроз, снижая вероятность технических нарушений и экономических потерь. При внедрении подхода важно учитывать, что формирование индивидуальных маршрутов и управление доступом на основе анализа рисков и экономических факторов увеличивает нагрузку на вычислительные и сетевые ресурсы, особенно при большом числе пользователей, что требует обеспечения достаточного объёма вычислительных ресурсов.

Полноценная защита подразумевает интеграцию SDP с SPA (Single Packet Authorization) методом обеспечения безопасности, который предоставляет доступ к запрашиваемому ресурсу только после получения информационного пакета, содержащего необходимые сведения для аутентификации. В отличие от традиционных многоэтапных методов, использование SPA упрощает процесс проверки за счёт применения ряда криптографических механизмов и правил брандмауэра, скрывающих внутренние сервисы до момента успешной авторизации.

Также предлагается дополнительное использование групповых политик безопасности, регламентирующих объём вычислительных ресурсов (таких, как размер выделяемой оперативной памяти в рамках RDP-сессии, процент выделенных ресурсов ЦП, лимитирование пропускной способности дисковой подсистемы) для приоритизации соединений в зависимости от степени значимости подключения. Данные механизмы могут быть реализованы посредством динамического создания и управления объектами групповых политик средствами операционных систем.

Сетевое взаимодействие может регламентироваться посредством аппаратно-программных маршрутизаторов (шлюзов) и управляемых коммутаторов L2+/L3 уровней модели OSI, управляющих прохождением трафика как в рамках организации, так и контролирующей межсетевую передачу данных с помощью механизмов инкапсуляции/декапсуляции сетевых пакетов, глубинного анализа трафика (DPI) и динамически конфигурируемых моделей реагирования в зависимости от аппаратной нагрузки и степени загруженности/пропускной способности каналов передачи данных.

В предлагаемом подходе, связывающем SDP, SPA, групповые политики безопасности и методы управления сетевым взаимодействием, каждый аутентификационный пакет данных уникален и предназначен исключительно для адресата. Брандмауэр на стороне внутреннего периметра безопасности анализирует пакет, проверяет подлинность учетных данных и предоставляет доступ только при их действительности. Такой механизм исключает возможность сканирования портов, блокируя доступ к внутренней инфраструктуре до момента успешной аутентификации. Совместное использование SDP и SPA создаёт гибкую модель адаптивного управления доступом.

Общая схема взаимодействия в рамках предлагаемого подхода включает несколько этапов. При подключении из внешней сети устройства сотрудника, которому необходимо получить доступ к терминальному серверу, в первую очередь осуществляется процесс идентификации, аутентификации и авторизации посредством программно-аппаратного комплекса SPA/SDP. Сетевое взаимодействие регламентируется правилами прохождения трафика, установленными на сетевом шлюзе, связывающем внутреннюю (локальную) сеть предприятия (ЛВС) и внешние каналы связи. При этом не является существенной как физическая, так и логическая сетевая топология. Количество промежуточных узлов от устройства сотрудника до шлюза организации не имеет значения при условии, что транзитные точки маршрутизации не осуществляют модификацию криптографически закрытого пакета данных. Последнее контролируется при помощи механизмов АН/ESP, анализирующих инкапсулированные в пакете данные с помощью хэширования посредством семейства алгоритмов SHA. При получении аутентификационного пакета модуль SDP осуществляет верификацию на предмет подмены/повреждения инкапсулированных данных. Если данный этап проходит успешно, то после дешифровки закрытым ключом проверяется — имеет ли право доступа к терминальному серверу устройство/сотрудник с указанными идентификационными и аутентификационными данными, а также вводится значение приоритета, определяющего пул ресурсов, которые будут выделены для туннельного соединения. В указанное понятие входит ширина сетевого канала, контролируемого механизмами QoS, объём вычислительных ресурсов терминального сервера, а также допустимое количество передаваемого и принимаемого сетевого трафика в рамках фиксированного периода.

В предложенном подходе протокол SDP формирует динамический и персонализированный внутренний периметр безопасности, скрывая инфраструктуру до момента успешной аутентификации, а SPA обеспечивает проверку подлинности с помощью единственного криптографически закрытого пакета. Дополнительно комбинация SDP и SPA позволяет заранее ограничивать потенциальные векторы угроз и повышать устойчивость инфраструктуры к распределённым botnet-атакам. Это обеспечивает не только высокий уровень информационной безопасности, но и повышение экономической эффективности терминальной инфраструктуры, снижая риски атак и избыточного использования ресурсов. Таким образом, применение модели SDP/SPA представляет собой перспективный подход к обеспечению информационно-экономической безопасности при использовании терминальных технологий.

#### СПИСОК ЛИТЕРАТУРЫ

1. Аминов Х.И. Методологические основания технологических инноваций цифровой экономики /Аминов Х.И., Верзун Н.А., Коршунов И.Л. и др. СПб: СПбГЭУ, 2023 203 с.
2. Верзун Н.А. Модели цифровой опасности в кибернетическом и когнитивном пространствах: колл. монография / Астахова Т.Н., Беломестнова Н.В., Верзун Н.А., Емельянов А.А. и др. Санкт-Петербург: Изд-во СПбГЭУ, 2023.
3. Демидов А.В., Емельянов А.А. Анализ уязвимостей и разработка требований к безопасности в современной IT-инфраструктуре // Цифровые опасности информационного общества. СПб: Изд-во СПбГЭУ, 2023. С. 42-48.
4. Емельянов А.А., Коршунов И.Л. Технические риски предприятия, связанные с цифровой трансформацией // Изв. вузов. Приборостроение. 2024. Т. 67. № 2. С. 116-121.

УДК 656.1:338.47(985)(519.86)

#### ТРАНСПОРТНО-ЛОГИСТИЧЕСКАЯ СИСТЕМА ЭСТАКАДНОГО ТИПА uST КАК СТРАТЕГИЧЕСКОЕ РЕШЕНИЕ ДЛЯ АРКТИКИ: ИНЖЕНЕРНЫЕ И СОЦИАЛЬНО-ЭКОНОМИЧЕСКИЕ АСПЕКТЫ

**Ерофеевский Даниил Владимирович, Митко Арсений Валерьевич**

Санкт-Петербургский государственный университет

Университетский пр., 28, Петергоф, Санкт-Петербург, 198504, Россия

e-mails: daniil.erofeevskii@yandex.ru, arseny73@yandex.ru

**Аннотация.** В работе рассматривается проект строительства транспортно-логистического комплекса uST на участке поселок Сабетта — город Надым в Арктической зоне Российской Федерации. Обосновывается стратегическая значимость проекта для устойчивого развития ЯНАО и Арктики в целом. Проведён анализ климатических и инженерных условий, дана сравнительная характеристика uST и традиционных транспортных решений. С использованием методов многокритериального анализа (АНР, TOPSIS) показано, что uST обеспечивает минимальные эксплуатационные издержки, высокий срок службы и низкое воздействие на экосистему. Проект подтверждает устойчивость к климатическим и экономическим рискам и формирует основу для долгосрочной транспортной связанности Арктики.

**Ключевые слова:** Арктика; транспортно-логистическая система; uST; Сабетта–Надым; АНР; TOPSIS; устойчивое развитие.

#### TRANSPORT AND LOGISTICS SYSTEM OF THE OVERPASS TYPE uST AS A STRATEGIC SOLUTION FOR THE ARCTIC: ENGINEERING AND SOCIO-ECONOMIC ASPECT

**Erofeevskii Daniil, Mitko Arseniy**

Saint Petersburg State University

28 University Av., Peterhof, St. Petersburg, 198504, Russia

e-mails: daniil.erofeevskii@yandex.ru, arseny73@yandex.ru

**Abstract.** The paper examines the project of constructing a uST transport-logistics complex on the Sabetta — Nadym section in the Arctic Zone of the Russian Federation. The strategic importance of the project for sustainable development of Yamal-Nenets Autonomous Okrug and the Arctic as a whole is substantiated. The study analyzes climate and engineering conditions and provides a comparative assessment of uST versus traditional transport solutions. Using multi-criteria analysis methods (AHP, TOPSIS), it is shown that uST ensures minimal operating costs, long service life and low impact on ecosystems. The project demonstrates resilience to climatic and economic risks and forms the basis for long-term Arctic connectivity.

**Keywords:** Arctic; transport-logistics complex; uST; Sabetta-Nadym; AHP; TOPSIS; sustainable development.

Развитие Арктической зоны Российской Федерации до 2035 года определено в стратегических документах как одно из ключевых направлений пространственного развития страны. Одним из наиболее острых вызовов является низкая транспортная связанность: плотность дорог в ЯНАО составляет менее 10 км на 1000 км<sup>2</sup> против более 100 км по России в среднем. Это приводит к высокому удорожанию перевозок, росту издержек домохозяйств и снижению инвестиционной привлекательности региона [1].

Исторический опыт эксплуатации автомобильных и железных дорог на вечномёрзлых и заболоченных грунтах показывает их низкую устойчивость. Деформации земполотна, просадки, солифлюкция и термокарст делают эксплуатацию традиционной инфраструктуры чрезвычайно затратной. Ремонтные работы на трассах Ямала ведутся ежегодно, стоимость содержания дорог в 3–5 раз выше, чем в регионах без мерзлоты. Технология Unitsky String Technologies (uST) основана на использовании эстакадных рельсо-струнных конструкций, размещённых на свайных фундаментах, уходящих в устойчивые слои грунта. Данное инженерное решение исключает прямое воздействие на верхние слабонесущие грунты, минимизирует земляные работы и снижает экологический ущерб. Подвижной состав — энергоэффективные беспилотные юнимобили — обеспечивает круглогодичное сообщение [2, 3].

Многокритериальный сравнительный анализ (MCDA), проведён методами AHP и TOPSIS. А также проведено сравнение сценариев строительства струнно-линейной эстакады uST с традиционными решениями: автомобильная дорога, железная дорога (ЖД) и зимник. В методе AHP (Analytic Hierarchy Process) были проведены попарные сравнения критериев: капитальные и эксплуатационные затраты, срок службы, энергоэффективность, землеотвод, выбросы CO<sub>2</sub>, надёжность, социальный эффект) показали, что ключевыми факторами для Арктики являются эксплуатационные затраты (15,5%), капитальные вложения (14,3%) и срок службы (14,1%). Существенную роль играют и социальные показатели (23,9%) — надёжность круглогодичной связи и вклад в развитие региона. В методе TOPSIS при ранжировании альтернатив (автодорога, железная дорога, зимник, uST) по степени приближения к идеальному решению uST занял первое место ( $C^* = 0,91$ ), существенно опередив железную дорогу (0,57), автодорогу (0,45) и зимник (0,21). Это подтвердило превосходство uST по совокупности экономических, экологических и эксплуатационных параметров. При DEA-анализе построенные границы эффективности показали, что uST находится на фронтире, тогда как автодорога и железная дорога демонстрируют существенное отставание по коэффициенту эффективности (0,62–0,75 против 1 у uST). С учётом экологических факторов (землеотвод, выбросы CO<sub>2</sub>, влияние на гидрологию) uST подтвердил статус наиболее устойчивой альтернативы: показатель эффективности составил 0,96 против 0,54 у железной дороги и 0,41 у автодороги.

Проведённое сценарное моделирование подтвердило устойчивость проекта в условиях климатических и экономических рисков. Рассмотрены базовый сценарий, ESG-сценарий, сценарий климатических рисков и экономического стресса. Даже при росте капитальных затрат на 15–20% и усилении деградации мерзлоты проект сохраняет положительное значение NPV, тогда как традиционные дороги становятся убыточными. Во всех сценариях uST остаётся устойчивым проектом, в то время как традиционные решения (автомобильная дорога, ЖД, зимник) демонстрируют высокую зависимость от климатических и экономических факторов. Наибольший разрыв в эффективности наблюдается при сценарии климатических рисков: эксплуатационные расходы на автодорогах возрастают в 4–5 раз, тогда как у uST сохраняются в пределах плановых. ESG-сценарий усиливает конкурентное преимущество uST, поскольку он изначально проектировался с минимальным воздействием на окружающую среду. Экономический кризис лишь снижает рентабельность, но не делает проект убыточным (в отличие от альтернативных видов транспорта). Социальный риск нивелируется за счёт многофункциональности uST (совмещение пассажирских и грузовых перевозок) [4, 5].

Таким образом, строительство транспортно-логистического комплекса uST на участке Сабетта — Надым обеспечивает:

- снижение капитальных затрат на 30–60% и операционных — до 70% по сравнению с традиционными трассами;
- минимизацию экологического воздействия (снижение выбросов CO<sub>2</sub> и землеотвода до 90%);
- круглогодичное и надёжное транспортное сообщение, устойчивое к сезонным колебаниям климата;
- стратегический вклад в социально-экономическое развитие ЯНАО и всей Арктической зоны РФ.

Результаты анализа однозначно показывают, что uST не является просто альтернативным видом транспорта, а представляет собой стратегическую инженерную инновацию, обеспечивающую надёжность, экономичность и экологичность транспортного сообщения в Арктике. Проект на участке Сабетта — Надым способен стать пилотной моделью тиражирования для всей Арктической зоны Российской Федерации.

## СПИСОК ЛИТЕРАТУРЫ

1. Вакуленко С. Ледяной фронт: роль Арктики в мировой энергетике [Электронный ресурс] // Carnegie Endowment. 2025. URL: <https://carnegieendowment.org/research/2025/07/arctic-energy> (дата обращения: 25.08.2025).
2. Куландин Д.А. Транспортно-логистическое развитие Ямало-Ненецкого автономного округа // Universum: технические науки. 2023. №6(111).
3. Юницкий А.Э., Филиппов Д.В., Рязанцев А.Н. Развитие транспортной системы в условиях высокоплотной застройки (на примере г. Мурино) // Вестник Сибирского государственного индустриального университета. 2023. № 4 (46). С. 124–134.
4. Hjørt J., Karjalainen O., Aalto J. et al. Degrading permafrost puts Arctic infrastructure at risk by mid-century // Nature Communications. 2018. Т.9. №5147.
5. Staalesen A. Moscow revives plans for a railway to Arctic coast at Sabetta // Arctic Today. 2021. June 11.

УДК 004.9, 334.025

**ЭКОНОМИКА КИБЕРБЕЗОПАСНОСТИ — ОДИН ИЗ ПРИОРИТЕТОВ ЦИФРОВОЙ  
ТРАНСФОРМАЦИИ ПРЕДПРИЯТИЯ**

**Коршунов Игорь Львович, Микадзе Сергей Юрьевич, Соловьева Янита Константиновна**

Санкт-Петербургский государственный экономический университет

Садовая ул., 21, Санкт-Петербург, 191023, Россия

e-mails: kil53@mail.ru, mik@finec.ru, yanita.solovieva@mail.ru

**Аннотация.** Цифровая трансформация предприятия связана с возрастанием роли кибербезопасности в деятельности предприятия. Особенности киберугроз в последнее время. Роль экономики кибербезопасности в цифровой трансформации. Характеристика проблем, возникающих при создании системы кибербезопасности на предприятии. Суть консервативного подхода к оценке системы кибербезопасности предприятия, обоснование необходимости перехода к прогрессивному подходу. Суть комплаенс-ориентированного подхода к оценке и управлению системой кибербезопасности предприятия, обоснование необходимости перехода к риск-ориентированному подходу.

**Ключевые слова:** кибербезопасность; цифровая трансформация предприятия; экономика кибербезопасности; прогрессивный подход к оценке системы кибербезопасности; риск-ориентированный подход к оценке и управлению кибербезопасностью.

**CYBERSECURITY ECONOMICS IS ONE OF THE PRIORITIES  
OF DIGITAL TRANSFORMATION FOR ENTERPRISES**

**Korshunov Igor, Mikadze Sergey, Solovyova Yanita**

St. Petersburg State University of Economics

21 Sadovaya St, St. Petersburg, 191023, Russia,

e-mail: kil53@mail.ru, mik@finec.ru, yanita.solovieva@mail.ru

**Abstract.** The digital transformation of an enterprise is associated with an increase in the role of cybersecurity in the enterprise's activities. Features of cyber threats in recent times. The role of cybersecurity economics in digital transformation. Characteristics of the problems that arise when creating a cybersecurity system at an enterprise. The essence of a conservative approach to assessing an enterprise's cybersecurity system, and the rationale for transitioning to a progressive approach. The essence of a compliance-oriented approach to assessing and managing an enterprise's cybersecurity system, and the rationale for transitioning to a risk-oriented approach.

**Keywords:** cybersecurity; digital transformation of an enterprise; cybersecurity economics; a progressive approach to assessing a cybersecurity system; and a risk-based approach to assessing and managing cybersecurity.

Происходящая в мире цифровая трансформация всех видов деятельности, в частности в России, переход к цифровой экономике и экономике данных, привела к переносу части бизнес-процессов предприятий в виртуальную среду, которая получила название «киберпространство» [1]. Предоставляя человеку новые колоссальные возможности работы с информацией, она, в то же время, может являться источником очень серьезных опасностей для предприятия. Согласно отчёту WEF Global Cybersecurity Outlook 2025 [2], ключевые риски сегодня связаны с геополитической напряжённостью, сложными цепочками поставок, внедрением новых технологий и ростом роли ИИ. Атаки теперь не просто нарушают работу инфраструктуры, но могут угрожать жизни людей и устойчивости общества.

Количество кибератак на предприятия растёт с каждым годом. В последнее время целью атак на российские объекты является не только получение экономической выгоды, но и нанесение любого вида ущерба (финансового, репутационного, морального и др.) любому российскому объекту, не считаясь с затратами на реализацию кибератаки [3]. В связи с этим вопросы создания системы кибербезопасности на предприятии (не только относящимся к объектам критической информационной инфраструктуры) являются актуальными, как для крупных предприятий, так и для малых.

Новые цели кибератак на российские предприятия, отмеченные выше (нанесение любого ущерба), выдвигают на первый план вопросы, связанные с экономикой кибербезопасности. Создание и обслуживание системы кибербезопасности на предприятии стоит дорого, а эффективность ее оценить сложно. Кроме того, в новых условиях требует пересмотра основной принцип экономической оценки разрабатываемой системы



кибербезопасности предприятия: на взлом системы безопасности хакер должен потратить средств больше, чем он получит в результате успешной кибератаки.

Экономика кибербезопасности предприятия рассматривает вопросы, связанные с изучением экономических аспектов защиты информационных ресурсов и информационной инфраструктуры предприятия от киберугроз: оценка рисков, управление затратами, распределение ресурсов, принятие решений в области кибербезопасности и др. Оценка рисков включает анализ уязвимостей, оценку возможных последствий атак, разработку стратегий минимизации рисков. Управление затратами предполагает решение задачи оптимизации расходов на обеспечение кибербезопасности за счет выбора наиболее эффективных методов и инструментов защиты, а также расчёт стоимости потенциальных потерь в результате успешных атак. Распределение ресурсов обеспечивает эффективное использование финансовых, технических, людских ресурсов в рамках существующей (создаваемой) системы кибербезопасности предприятия. Основой для принятия решений должен являться баланс между уровнем защищенности предприятия и стоимостью реализации мер защиты, т.е. основой стратегии кибербезопасности предприятия должна быть ее экономическая целесообразность.

При создании системы кибербезопасности на предприятии и оценки ее экономической эффективности сегодня существует ряд проблем. Во-первых, реализация производственной деятельности в киберпространстве предполагает значительное увеличение международных киберугроз, т.е. кибератаки могут осуществляться из любой точки мира. Во-вторых, переход на отечественные средства защиты, с одной стороны, ограничивает выбор инструментов защиты, а с другой, затрудняет его, т.к. отсутствует подробная достоверная информация о продуктах, которые включены в Реестр российского ПО, и особенностях (опыте) их применения. В-третьих, на большинстве российских предприятий отсутствует система контроля и управления использованием средств кибербезопасности. По данным Всемирного банка [4], сегодня в мире 66 % инцидентов не обнаруживаются в первые 30 дней, а 69 % выявляются извне, что указывает на значительные недооценённые потери. Для решения перечисленных проблем необходима активная деятельность государства в определении подходов к оценке систем кибербезопасности предприятий, в оказании помощи по навигации в Реестре российского ПО для правильного выбора инструментов для конкретного предприятия, особенно не имеющего опыта создания подобных систем. Особо следует отметить необходимость решения вопроса о легализации в стране деятельности «белых хакеров», что позволит оценивать систему кибербезопасности предприятия по результатам испытания ее в реальной ситуации.

Сегодня в нашей стране для оценки системы кибербезопасности предприятия государство реализует консервативный подход. Его суть заключается в минимизации рисков путем реализации защитных мер на основе принципа «лучше перестраховаться, чем потом жалеть». Особенности данного подхода являются: минимизация угроз, предсказуемость поведения системы, максимальная защита, осторожность и осмотрительность. Минимизация угроз обеспечивается за счет ограничения доступа к критически важным ресурсам и данным, использования проверенных и надежных технологий защиты, регулярной проверки и обновления всех компонентов системы защиты. Предсказуемость поведения системы предполагает применение стандартизированных процедур и политик безопасности, минимизацию количества изменений конфигураций и внедрения новых технологий. Максимальная защита строится на многослойности обороны («defense in depth»), реализации принципов «нулевого доверия» и минимальной привилегии. Осторожность и осмотрительность включает в себя исключение неоправданных рисков и нововведений без достаточного обоснования, осторожное отношение к новым технологиям и решениям до проверки их временем и практическим опытом. Для оценки эффективности системы кибербезопасности при рассматриваемом подходе используются следующие методы: риск-анализ, тестирование и аудит, мониторинг и реагирование. Преимуществами консервативного подхода являются: высокая степень защищенности объекта, надежность и предсказуемость поведения системы, снижение риска серьезных инцидентов. Основным недостаток данного подхода — сложность адаптации к быстро меняющимся угрозам. В условиях быстрого развития информационных технологий и появления новых угроз данный подход не позволяет быстро реагировать на происходящие изменения. Существуют альтернативные подходы к оценке системы кибербезопасности предприятия, например: инновационный, агрессивный, сбалансированный, динамический и др.

В сложившейся ситуации целесообразно использовать прогрессивный подход, который ориентирован на гибкость и адаптивность к новым технологиям, на быстро меняющийся ландшафт киберугроз. Его ключевыми элементами являются: использование передовых технологий, непрерывное совершенствование процессов, аналитика и предиктивное моделирование, коллаборация и партнерство. Искусственный интеллект и машинное обучение, автоматическое управление идентификацией и доступом, биометрическая аутентификация и многофакторная авторизация — это основные технологии, которые применяются в рамках прогрессивного подхода. Совершенствование процессов происходит за счет постоянного мониторинга и оценки состояния безопасности, построения культуры безопасности внутри предприятия и проведения «кибергигиены», разработки и реализации планов непрерывности бизнеса и восстановления после инцидентов. Аналитика и предиктивное моделирование предполагают сбор и анализ большого объема данных для выявления закономерностей и тенденций, для прогнозирования будущих угроз и разработки превентивных мер. Сотрудничество с поставщиками услуг кибербезопасности, исследовательскими институтами и государственными структурами, участие в международных инициативах и обмен информацией о киберугрозах являются неотъемлемыми элементами прогрессивного подхода.

Прогрессивный подход обладает большей эффективностью в борьбе с новыми видами угроз, повышает общую готовность предприятия к негативным событиям, обладает гибкостью и способностью адаптироваться к изменениям рынка. Автоматизация многих процессов в рамках этого подхода снижает риск ошибок и повышает надежность системы. Однако для успешного внедрения прогрессивного подхода необходимы значительные инвестиции в технологии, персонал и процессы управления кибербезопасностью.

Еще один подход, реализуемый сегодня в нашей стране на законодательном уровне для оценки и управления системой кибербезопасности предприятия — это комплаенс-ориентированный подход. Его цель — обеспечить соответствия требованиям нормативных актов, стандартов и внутренних регламентов. Он акцентирует внимание на соблюдении правил и требований регулирующих органов, на предотвращении правовых последствий нарушений законодательства. Реализация формализованного процесса позволяет определить степень соответствия системы безопасности законодательным требованиям и сравнить системы безопасности различных предприятий. В современных условиях данный подход может привести к недооценке реальных рисков. Он не учитывает особенности конкретного предприятия и характеризуется высоким уровнем бюрократизации процесса и длительной процедурой аттестации и подтверждения соответствия. Комплаенс-ориентированный подход сегодня в профессиональных кругах неофициально называют «бумажной безопасностью», он не позволяет обеспечить эффективное предотвращение угроз. Альтернативой данному подходу может служить риск-ориентированный подход. Он основан на систематическом анализе рисков использования информационных технологий и разработке мер по их устранению или минимизации. Он ориентирован на выявление реальных угроз и уязвимостей, характерных для конкретного предприятия. Основная цель данного подхода состоит в обеспечении эффективного распределения ресурсов для снижения наиболее значимых рисков, обеспечивая приемлемый уровень кибербезопасности. Реализация данного подхода предполагает выполнение следующих этапов: идентификация рисков, оценка рисков, приоритезация рисков, планирование и реализация мер по снижению рисков, мониторинг и контроль. Риск-ориентированный подход позволяет более рационально распределять финансовые и человеческие ресурсы, эффективнее применять меры по повышению уровня безопасности, сосредоточиться на устранении наиболее важных угроз. Сложности реализации данного подхода связаны с необходимостью регулярного обновления базы знаний о существующих угрозах и уязвимостях, наличием высококвалифицированных кадров в области кибербезопасности. В условиях динамично развивающихся угроз применение риск-ориентированного подхода становится необходимым условием успешной борьбы с киберпреступностью и обеспечением стабильной работы предприятий.

Таким образом, экономика кибербезопасности, являясь неотъемлемой частью цифровой трансформации предприятия, требует применения новых подходов к оценке систем кибербезопасности предприятия.

#### СПИСОК ИСТОЧНИКОВ

1. Модели цифровой опасности в кибернетическом и когнитивном пространствах : коллективная монография / под ред. М.О. Колбанёва, И.Л. Коршунова. СПб. : Изд-во СПбГЭУ, 2023. 194 с. EDN DCWEVT.
2. Доклад WEF Global Cybersecurity Outlook 2025. <https://industrialcyber.co/reports/wef-global-cybersecurity-outlook-2025-report-addresses-geopolitical-tensions-emerging-threats-to-boost-resilience/> (дата обращения: 15.08.2025).
3. ПМЭФ-2025. Экономика кибербезопасности: стратегические приоритеты системообразующих предприятий и инновации в киберустойчивость. <https://forumspb.com/programme/business-programme/145651/> (дата обращения: 15.08.2025).
4. Estefania Vergara Cobos. Cybersecurity economics for emerging markets / International Bank for Reconstruction and Development / The World Bank 2024. <https://documents1.worldbank.org/curated/en/099091624175097991/pdf/P17876915bd69a0671b2f2166697a1c7793.pdf> (дата обращения: 15.08.2025).

УДК 004.9, 334.025

#### РИСКИ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЭКОНОМИКЕ

**Коршунов Игорь Львович, Тумарев Владимир Михайлович, Шумаева Алина Денисовна**

Санкт-Петербургский государственный экономический университет

Садовая ул., 21, Санкт-Петербург, 191023, Россия

e-mails: kil53@mail.ru, vladimir13@inbox.ru, alinashumaeva1@gmail.com

**Аннотация.** Технологии искусственного интеллекта активно внедряются во все сферы жизни, демонстрируя отличные результаты при решении сложных задач. Вместе с тем, их использование несет в себе колоссальные риски для экономики, общества и человека, о которых сегодня мало говорят. Понятие ИИ, функции интеллектуальной системы. Особенности применения ИИ в экономике. Экономические, социальные и технические риски использования ИИ в экономике. Проблема «черного ящика» при использовании ИИ в экономике. Особенности отечественных моделей ИИ.

**Ключевые слова:** искусственный интеллект; модели ИИ; риски использования ИИ в экономике; проблема «черного ящика» в ИИ; российские модели ИИ.

#### RISKS OF USING ARTIFICIAL INTELLIGENCE IN THE ECONOMY

**Igor Korshunov, Vladimir Tumarev, Alina Shumaeva**

St. Petersburg State University of Economics

21 Sadovaya St, St. Petersburg, 191023, Russia

e-mails: kil53@mail.ru, vladimir13@inbox.ru, alinashumaeva1@gmail.com

**Abstract.** Artificial intelligence technologies are actively being introduced into all areas of life, demonstrating excellent results in solving complex problems. However, their use poses enormous risks to the economy, society, and individuals, which are often overlooked. The concept of AI and the functions of an intelligent system. The specific features of AI applications in the economy. The economic, social, and technical risks associated with the use of AI in the economy. The «black box» problem in the use of AI in the economy. The characteristics of domestic AI models.

**Keywords:** artificial intelligence; AI models; risks of using AI in the economy; the «black box» problem in AI; Russian AI models

Анализ публикаций как в средствах массовой информации, так и в научных изданиях позволяет утверждать, что тема ИИ является самой востребованной. В первую очередь это связано с мощным развитием соответствующих технологий, которые становятся ключевыми факторами экономики, науки и политики. Они демонстрируют хорошие результаты при решении сложных задач, а также проникают в повседневную жизнь, демонстрируя повышение эффективности реализуемых процессов. С другой стороны, внедрение технологий ИИ влечет за собой колоссальные риски для всего общества, масштаб которых пока еще не определен. Неоправданно много хвалебных отзывов об ИИ звучит от политиков и экономистов, ИТ-специалисты осторожней в своих суждениях. В связи с этим, говоря о рисках применения ИИ, следует различать опасности использования ИИ-технологий в предметной области и опасности самих ИИ-технологий.

Исторически понятие «искусственный интеллект» появилось в рамках науки, которая называется кибернетика. Уже тогда ученые связали его со знаниями и определили его как технологии решения задач, опирающиеся на идею использования знаний о предметной области [1]. За прошедшие годы мнение ученых (кибернетиков) не изменилось, но появились новые подходы, например, биологический и трансдисциплинарный. Авторы данного доклада придерживаются кибернетического подхода и разделяют мнение коллег, что знания являются ядром интеллектуальной системы, а их свойства (полнота, корректность и др.) и методы работы с ними — определяют потенциальные возможности конкретной интеллектуальной системы. По сути любая интеллектуальная система выполняет три основные функции: получение знаний, представление знаний и использование знаний. Все технологии ИИ, успешно используемые сегодня в нашей жизни, могут быть отнесены к одной из этих трех групп. Источником знаний являются разнообразные данные, разработаны методы и алгоритмы получения знаний из данных, они реализуются в виде программных инструментов и приложений. Полученные знания необходимо представить в виде структур, для этого используются формальные языки, позволяющие автоматически транслировать тексты в машиночитаемую или машинопонимаемую форму. Наиболее распространенной сегодня является модель представления знаний в виде семантической сети. Использование знаний предполагает решение конкретных задач в предметной области. На основе разработанных методов, алгоритмов и инструментов создается технология, которая представляет собой приложение для интеллектуальной системы. Это наиболее многочисленная группа ИИ-технологий, входящие в нее технологии связаны с конкретными сферами деятельности (нейросетевые технологии, компьютерное зрение, обработка естественного языка и др.). Таким образом, деятельность интеллектуальных систем связана с использованием значительного количества технологий, реализуемых в виде программных продуктов. Ошибки, допущенные в методах, алгоритмах, программных кодах, могут накапливаться и давать неверный результат решения прикладной задачи.

Внедрение ИИ в экономику характеризуется кардинальной трансформацией привычных экономических процессов, появлением новых возможностей для роста производительности, повышения эффективности и инноваций, изменением рынка труда. В качестве положительных моментов интеграции ИИ в отрасли экономики можно отметить следующие: повышение продуктивности и автоматизации процессов, улучшение аналитики больших объемов данных, персонализация товаров и услуг, оптимизация цепей поставок, создание новых бизнес-моделей и рынков. Наряду с отмеченными достоинствами интеграции ИИ в экономику, следует иметь в виду, что этот процесс требует тщательного планирования, значительных финансовых вложений в ИТ-инфраструктуру, наличия квалифицированных специалистов, а также внимательного подхода к вопросам этики и безопасности. Интеграция ИИ в экономику несет в себе серьезные риски, масштабы которых пока еще не могут быть оценены полностью. По характеру проявления широкий спектр рисков можно объединить в три группы ключевых рисков: экономические, социальные и технические. Экономические риски представляют угрозу экономической устойчивости и могут проявляться в потере контроля понимания экономических процессов, в изменении структуры и «переформатировании» экономики. Внедрение ИИ в экономику усложняет существующую систему управления экономикой, делает ее непонятной для общественного понимания. Принятие решений ИИ, особенно в кризисных ситуациях, очень опасно, если отсутствует объяснение логики действия системы. Данная опасность сегодня существует — это проблема «черного ящика». Структурные риски и «переформатирование» экономики — это фундаментальный и наименее очевидный риск, он проявляется в том, что ИИ не просто меняет инструменты, а кардинально трансформирует экономические структуры. Меняется природа конкуренции, управление и создание стоимости, происходит монополизация и концентрация власти, ограничивающая перспективы малых и средних предприятий. Социальные риски связаны с потерей рабочих мест и изменением структуры занятости, с дискриминацией и усилением предвзятости. Автоматизация производственных процессов с использованием ИИ ведет к исчезновению многих профессий, не только рабочих, но и специальностей, которые связаны с выполнением рутинных операций — это приведет к росту социальной напряженности в обществе.

Алгоритмы ИИ при обучении на субъективных данных могут воспроизводить и усиливать предвзятости человека-владельца данных, например, занижать рейтинги заемщиков определенных социальных групп, не принимать на работу кандидатов определенного пола или расы. Технические риски обусловлены используемыми аппаратно-программными средствами для реализации технологий ИИ и тесно связаны с кибербезопасностью. Системы ИИ работают с огромными объемами данных, уязвимости в их защите создают предпосылки для мошенничества и злоупотребления их использованием. Технические риски связаны также с необходимостью значительных инвестиций на внедрение технологий ИИ, создание сложных моделей ИИ требует серьезных финансовых затрат. Существуют также риски операционных сбоев, как у любой сложной технической системы, поэтому нужны финансовые затраты на резервирование аппаратных средств и переход на ручное управление.

Проблема «черного ящика» является сегодня серьезным риском, существенно ограничивающим использование ИИ в критически важных областях экономики. Суть ее состоит в отсутствии объяснения логики принятия решения ИИ. Это приводит к снижению доверия к технологии, даже если она эффективно работает и выдает правильные результаты. Причинами данной проблемы считаются сложность моделей, их нелинейность и нелинейная природа данных, а также присутствие автоматического обучения. Современные модели глубокого обучения (сверточные нейронные сети, трансформеры) содержат миллионы слоев и параметров, что делает их чрезвычайно сложными для понимания и анализа даже разработчиками. Работа с нелинейными преобразованиями данных серьезно затрудняет выявление четких закономерностей между входными данными и выходными результатами. Алгоритмы автоматического обучения, как правило, реализуют методы оптимизации, которые вызывают сложности при интерпретации. Кроме того, непрозрачность моделей может скрывать уязвимости, открывающие возможности для злонамеренных кибератак типа adversarial attacks [2], которые за счет незначительного изменения входных данных приводят к значительным изменениям результата. В настоящее время специалисты рассматривают следующие возможные направления решения описанной проблемы. Во-первых, это развитие методов объяснимого ИИ (Explainable AI, XAI), позволяющих человеку понять логику принятия решения ИИ. К данной группе методов относятся методы, не зависящие от модели (Model-agnostic). Они представляют собой интерпретационные техники (LIME, SHAP) [3], которые помогают интерпретировать предсказание любой сложной модели, аппроксимируя ее поведение с помощью более простых моделей или вклад каждого признака в общий результат. К рассматриваемой группе относятся также методы визуализации (салиентные карты — Saliency Maps), реализующие интерфейсы визуализации для наглядного представления внутреннего состояния модели. Вторым направлением решения проблемы «черного ящика» является разработка моделей с прозрачной структурой. В условиях, когда за счет незначительного снижения точности можно использовать более простую модель, предлагается применять интерпретируемые модели, построенные на базе деревьев решений или линейных моделей. Разработка стандартов и нормативных актов, требующих объяснения принимаемых решений, является еще одним направлением решения проблемы. Таким образом, проблема «черного ящика» представляет собой не просто техническую сложность, а комплексный вызов, находящийся на стыке технологии, этики, права и общественного доверия.

Ключевым моментом в развитии ИИ является создание моделей ИИ. Эта деятельность сопряжена с множеством технических и экономических трудностей, поэтому разработкой собственных фундаментальных базовых моделей на основе генеративного ИИ занимаются примерно в десяти странах, в том числе и в России.

Отечественные методы обучения моделей искусственного интеллекта, несмотря на отставание от западных лидеров в некоторых аспектах, демонстрируют устойчивый прогресс и обладают уникальными особенностями, обусловленными российским научным опытом и культурными традициями. К ним относятся: математический фундаментализм, оптимизация ресурсоемкости, инновационный подход к обучению и фокус на прикладных задачах. Российская наука традиционно сильна в математике, поэтому отечественные разработчики моделей уделяют особое внимание строгому обоснованию используемых методов и глубокому пониманию внутреннего устройства моделей. Из-за ограниченности вычислительных ресурсов российские разработчики сосредотачивают внимание на применении методов, позволяющих добиться хороших результатов при минимальных затратах. Для сокращения отставания отечественные ученые активно экспериментируют с новыми архитектурами нейронных сетей и методами обучения, предлагая оригинальные идеи и концепции. Российские разработчики достигли определенных успехов в обработке текста и изображения. Мультимодальные модели (например, Janus-Pro от DeepSeek) способны генерировать изображения по текстовым описаниям и анализировать визуальный контент. Одним из важнейших направлений является внедрение платформ для управления процессами машинного обучения. Отечественная платформа Сайбокс [4] используется для управления всем циклом производства ИИ — от сбора данных и обучения моделей до внедрения и мониторинга. При создании отечественных моделей ИИ серьезное внимание уделяется вопросам кибербезопасности и требованиям регуляторики с целью обеспечения соответствия требованиям доверенного ИИ. При решении задач, требующих повышенного контроля над данными, разработчики ориентируются на on-premise решения [5]. С точки зрения технического решения, наши разработчики используют современные архитектуры моделей, например, случайные леса и деревья решений, нейронные сети. Завершая рассмотрение особенностей российских моделей ИИ, можно отметить, что они характеризуются адаптацией под локальные нужды, акцентом на управление жизненным циклом, ставкой на качество данных, широким использованием персонализации и соблюдением требований безопасности. Эти подходы позволяют создать конкурентоспособные решения, ориентированные на нужды рынка и общества.

В заключении следует отметить, что для снижения рисков использования ИИ в экономике следует сосредоточить усилия на совершенствовании технологий ИИ и снижении рисков их применения.

#### СПИСОК ИСТОЧНИКОВ

1. Городецкий В.И., Юсупов Р.М. Искусственный интеллект — наука и информационная технология: настоящее и будущее // Материалы конференции «Информационные технологии в управлении», 2020 г. С. 3-14. <https://itc.etu.ru/assets/files/itc-2020/papers/003.pdf> (дата обращения: 20.08.2025).
2. Введение в Adversarial attacks: как защититься от атак в модели глубокого обучения на транзакционных данных. <https://habr.com/ru/companies/vtb/articles/718024/> (дата обращения: 20.08.2025).
3. LIME, SHAP. <https://habr.com/ru/companies/otus/articles/779430/> (дата обращения: 20.08.2025).
4. Интегрированная среда разработки ML-моделей Сайбокс. <https://t1-solutions.ru/products/scibox> (дата обращения: 20.08.2025).
5. Архитектурные особенности on-premises продуктового решения. <https://habr.com/ru/articles/859740/> (дата обращения: 20.08.2025).

УДК 631.14

### МОДЕЛЬ ОЦЕНКИ ЦИФРОВОЙ ТРАНСФОРМАЦИИ СЕЛЬСКОГО ХОЗЯЙСТВА

Маслов Никита Сергеевич

Нижегородский государственный инженерно-экономический университет

Октябрьская ул., 22а, Княгинино, 606340, Россия

e-mail: j-knaginino@yandex.ru

**Аннотация.** В условиях цифровизации сельского хозяйства необходимы инструменты, позволяющие объективно оценивать уровень цифровой зрелости и формировать приоритеты развития. В работе предложен системный подход, основанный на модели, включающей ключевые направления цифровой трансформации сельского хозяйства.

**Ключевые слова:** цифровая трансформация; сельское хозяйство; цифровая зрелость; система оценки.

### MODEL OF DIGITAL TRANSFORMATION OF AGRICULTURE

Maslov Nikita

Nizhny Novgorod State of Engineering and Economic University

5 Oktyabrskaya St, Knyaginino, 606340, Russia

e-mail: j-knaginino@yandex.ru

**Abstract.** The paper presents a system approach to assessing the digital maturity of agriculture. The methodology is based on a model that includes the main directions of digital transformation, enabling diagnostics of strengths, weaknesses and priority areas for development.

**Keywords:** digital transformation; agriculture; digital maturity; integrated model; assessment system.

Цифровизация рассматривается как ключевой фактор устойчивого развития и повышения конкурентоспособности сельского хозяйства. Однако цифровизация происходит неравномерно: в ряде регионов активно развиваются технологии точного земледелия и IoT, в то время как кадровое обеспечение и инновационная активность остаются на низком уровне [1]. Это предопределяет необходимость разработки комплексных инструментов оценки, которые позволят не только измерить уровень цифровой зрелости, но и выявить «слабые звенья» в системе.

Предложенный системный подход реализован в форме интегральной модели, включающей шесть взаимосвязанных блоков:

1. Технологии. Рассматривается спектр цифровых решений — от базовых информационных систем и электронного документооборота до высокотехнологичных платформ на основе искусственного интеллекта, и автоматизированных систем мониторинга.

2. Инфраструктура. Включает телекоммуникационные сети, устойчивое электроснабжение, облачные сервисы и центры обработки данных. Недостаток инфраструктурного обеспечения становится критическим ограничением даже при наличии финансирования и готовности хозяйств внедрять новые технологии.

3. Образование и кадры. Цифровая трансформация невозможна без квалифицированных специалистов. В модели учитывается уровень цифровой грамотности работников, наличие профильных образовательных программ и система повышения квалификации [2].

4. Государственная поддержка. Включает финансовые механизмы (субсидии, гранты, налоговые льготы), правовое регулирование и региональные программы. Данный блок играет роль катализатора цифровизации, особенно для хозяйств с низким уровнем инвестиционной активности.

5. Инновации и исследования. Отражают активность вузов, научных центров и бизнеса в разработке и внедрении новых решений. Учитываются показатели НИОКР, публикационная и патентная активность, участие в международных проектах.

6. Экономическая эффективность. Позволяет оценить влияние цифровизации на производительность, издержки, прибыль и устойчивость хозяйств. Также учитывается возврат инвестиций (ROI) и формирование новых моделей цифровой экономики в сельском хозяйстве.

Модель цифровой трансформации представляет собой универсальный инструмент диагностики цифровой зрелости сельского хозяйства [3]. Её применение дает возможность проводить межрегиональные сравнения, выявлять узкие места, а также формировать стратегические ориентиры цифровизации. Модель может использоваться как в отдельных хозяйствах, так и в региональном масштабе, что повышает её практическую значимость для развития аграрного сектора.

#### СПИСОК ЛИТЕРАТУРЫ

1. Zavivaev N. S., Yakimova O. Yu., Mansurov A. P. Klasternyj analiz effektivnosti ispol'zovaniya elementov tochnogo selskhozajstva [Cluster analysis of the efficiency of using elements of precision agriculture], Vestnik NGIEI [Bulletin of NGIEI], 2021, No. 12 (127), pp. 82–94, DOI 10.24412/2227-9407-2021-12-82-94, EDN PVNHHEM.
2. Bannikov S. A., Garbuzova T. G., Kovaleva T. N. Sushchnost' i etapy tsifrovoj transformatsii v APK [Essence and stages of digital transformation in the agro-industrial complex], Vestnik NGIEI [Bulletin of NGIEI], 2023, No. 11 (150), pp. 65–76, DOI 10.24412/2227-9407-2023-11-65-76, EDN GOJNZB.
3. Астахова Т. Н., Колбанев М. О., Шамин А. А. Децентрализованная цифровая платформа сельского хозяйства // Вестник НГИЭИ. 2018. № 6 (85). С. 5-17.

УДК 004.7

#### МАТЕМАТИЧЕСКАЯ МОДЕЛЬ СИСТЕМЫ АКУСТИЧЕСКОГО РАСПОЗНАВАНИЯ НЕИСПРАВНОСТЕЙ В РАБОТЕ ТЕХНИЧЕСКИХ ОБЪЕКТОВ

**Верзун Наталья Аркадьевна, Колбанёв Михаил Олегович, Салиева Аделина Рустамовна**

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

Профессора Попова ул., 5, Санкт-Петербург, 197022, Россия

e-mails: verzun.n@unecon.ru, mokolbanev@mail.ru, adelina\_salieva@mail.ru

**Аннотация.** Рассматривается акустическая система распознавания сбоев и отказов автономно функционирующих технических объектов — конвейеров, автомобилей, роботов и пр. Подобные системы должны своевременно и надежно распознавать неисправности на основе акустических сигналов, издаваемых работающим оборудованием. Процесс акустического распознавания представлен в виде двухфазной системы массового обслуживания. Предложены математическая модель системы и методы расчета вероятностно-временных характеристик процесса акустического распознавания неисправностей, позволяющие учитывать интенсивность поступающих звуковых событий, параметры их обработки, требования к времени реакции системы.

**Ключевые слова:** безопасность работы оборудования; акустическое распознавание; техническая диагностика; моделирование процесса распознавания.

#### MATHEMATICAL MODEL OF AN ACOUSTIC FAULT RECOGNITION SYSTEM FOR TECHNICAL OBJECTS

**Verzun Natalia, Kolbanev Mikhail, Salieva Adelina**

Saint Petersburg Electrotechnical University

5 Professor Popov St, St. Petersburg, 197022, Russia

e-mails: verzun.n@unecon.ru, mokolbanev@mail.ru, adelina\_salieva@mail.ru

**Abstract.** This paper discusses an acoustic fault and failure recognition system for autonomously operating technical objects such as conveyors, vehicles, robots, and similar equipment. Such systems must promptly and reliably detect faults based on acoustic signals emitted by operating machinery. The acoustic recognition process is represented as a two-phase queuing system. A mathematical model of the system is proposed, along with methods for calculating the probabilistic and temporal characteristics of the acoustic fault recognition process. These methods take into account the intensity of incoming acoustic events, their processing parameters, and the system's response time requirements.

**Keywords:** equipment operational safety; acoustic recognition; technical diagnostics; recognition process modeling.

Безопасность и надежность автономно функционирующего оборудования, а это могут быть роботы, конвейеры, транспортные средства и пр., зависит от своевременного и точного выявления и распознавания различных отклонений в работе механизмов до появления критических сбоев.

Перспективным направлением в этой сфере является внедрение акустических систем мониторинга, способных распознавать различные неисправности на основе анализа акустических сигналов, издаваемых оборудованием в процессе работы [1]. Возможность выявлять дефекты в работе оборудования еще на стадии зарождения особенно полезна.

Ранее авторами [2] был проведен анализ перспектив создания и применения систем акустического распознавания и предложены алгоритмы их работы на основе обучения с подкреплением. Предлагаемые алгоритмы [3] часто имеют высокую вычислительную сложность, и поэтому, для повышения быстродействия их работы, необходимо искать новые подходы к организации систем акустической диагностики, которые бы учитывали специфику предметной области и требования к скорости принятия решений об эксплуатационном состоянии оборудования.

В системах акустического распознавания для корректной диагностики состояния работающего оборудования используются звуковые сигналы, собираемые с помощью микрофонов от разных частей/узлов, при этом требования к скорости распознавания дефектов в их работе могут существенно различаться. Для надежной работы подобных систем в данном случае целесообразно использовать подход, позволяющий регулировать распределение ресурсов системы: для диагностики состояния критических узлов/агрегатов выделять больше вычислительных ресурсов, чем для менее критичных или второстепенных [4].

В докладе предлагается модель двухэтапной системы акустической диагностики. Первый этап — передача звуковых сигналов к устройству обработки и анализа сигнала, второй этап — непосредственно обработка звукового сигнала и принятие решения о состоянии работающего узла. При этом на каждом этапе предполагается гибкое деление общих ресурсов системы — канала передачи и процессора. Математическое моделирование процесса акустического распознавания основано на его представлении в виде двухфазной системы массового обслуживания вида M/G/1.

Предложены выражения, задающие математическую модель системы и разработаны методы расчета вероятностно-временных характеристик процесса акустического распознавания неисправностей, позволяющие учитывать интенсивность поступающих звуковых событий, параметры их обработки, требования к времени реакции системы и пр. [5].

Проведен численный расчет и анализ влияния параметров системы акустической диагностики при разных сценариях нагрузки на вероятностно-временные характеристики процесса распознавания неисправностей. Определены минимально необходимые характеристики (частота дискретизации, число параллельных обработчиков, время анализа сигнала и пр.) для обеспечения уровня безопасности.

Разработанная модель позволяет рассчитывать параметры акустической системы диагностики для условий, требующих высокой надежности и оперативности при мониторинге технического состояния объектов. Её применение даёт возможность обосновать требования к аппаратной и программной части систем технической диагностики, что особенно важно в контексте обеспечения промышленной безопасности и решении задачи продления ресурса оборудования.

#### СПИСОК ЛИТЕРАТУРЫ

4. Верзун Н.А., Колбанев М.О., Салиева А.Р. Многоагентный ансамблевый алгоритм акустического распознавания нарушений работоспособности автономного технологического оборудования // Информационно управляющие системы. 2025. Т.3., ISSN 1684-8853 (print); ISSN 2541-8610 (online) DOI: 10.31799.
5. Верзун Н. А., Колбанев М. О., Салиева А. Р. Анализ перспектив обучения умных автономных логистических систем на основе оптимизации функции ценности // Изв. СПбГЭТУ «ЛЭТИ». 2024. Т. 17, № 10. С. 28-39. doi: 10.32603/2071-8985-2024-17-10- 28-39.
6. Вишневецкий В. М. Теоретические основы проектирования компьютерных сетей. Москва: Техносфера, 2003. 512 с.
7. Верзун Н. А., Колбанев М. О., Коршунов И. Л., Микадзе С. Ю. Основы моделирования информационных систем множественного доступа. Санкт-Петербург: Санкт-Петербургский государственный экономический университет, 2015. 138 с.
8. Верзун Н. А., Колбанев М. О., Романова А. А., Цехановский В. В. Модель регулируемого множественного доступа в сети интернета вещей // Известия СПбГЭТУ ЛЭТИ. 2020. № 10. С. 20–27.

УДК 004.7

#### РАЗРАБОТКА И ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ МЕТОДА ОБУЧЕНИЯ С ПОДКРЕПЛЕНИЕМ ДЛЯ ЗАДАЧ АКУСТИЧЕСКОЙ ДИАГНОСТИКИ ПРОМЫШЛЕННОГО ОБОРУДОВАНИЯ

Салиева Аделина Рустамовна

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)  
Профессора Попова ул., 5, Санкт-Петербург, 197022, Россия  
e-mail: adelina\_salieva@mail.ru

**Аннотация.** Представлено исследование, направленное на разработку адаптивного метода акустической диагностики промышленного оборудования с использованием обучения с подкреплением (Reinforcement Learning, RL). Актуальность работы обусловлена необходимостью преодоления limitations традиционных методов на основе обучения с учителем, включая их зависимость от больших объемов размеченных данных, низкую адаптивность к изменяющимся условиям эксплуатации и отсутствие механизмов принятия решений в реальном времени. Предложенная методология основана на синтезе спектрального анализа акустических сигналов (БПФ, MFCC-коэффициенты) и RL-парадигмы. Разработанный метод включает: регистрацию и предобработку сигналов, извлечение информативных спектральных признаков, формирование RL-модели с формализацией состояния среды, действий и функции вознаграждения, а также механизм принятия диагностических решений. Экспериментальные исследования на верифицированных наборах данных (CWRU Bearing Data, MIMII Dataset, DCASE2020 Challenge) продемонстрировали высокую эффективность метода: точность классификации до 98,5%, время отклика 0,5-0,7 секунды при низкой вычислительной нагрузке (36,5% CPU, 509 МБ RAM). Результаты подтверждают практическую применимость метода для мониторинга состояния оборудования в условиях внешних шумов и нестационарности сигналов. Перспективные направления развития включают интеграцию с IoT-платформами, повышение устойчивости к шумам и внедрение продвинутых RL-алгоритмов.

**Ключевые слова:** акустическая диагностика; промышленное оборудование; обучение с подкреплением; RL-агент; спектральный анализ; предиктивное обслуживание; интеллектуальные системы мониторинга.

## DEVELOPMENT AND EXPERIMENTAL STUDY OF THE TRAINING METHOD WITH REINFORCEMENT FOR THE TASKS OF ACOUSTIC DIAGNOSIS OF INDUSTRIAL EQUIPMENT

Salieva Adelina

St. Petersburg State Electrotechnical University «LETI»

5 Professor Popov St, St. Petersburg, 197022, Russia

e-mail: adelina\_salieva@mail.ru

**Abstract.** A study is presented aimed at developing an adaptive method of acoustic diagnosis of industrial equipment using reinforcement learning (Reinforced Learning, RL). The relevance of the work is due to the need to overcome Limitations of traditional methods based on learning with the teacher, including their dependence on large amounts of the marked data, low adaptability to changing operating conditions and the absence of decision -making mechanisms in real time. The proposed methodology is based on the synthesis of the spectral analysis of acoustic signals (BPF, MFCC coefficients) and RL paradigms. The developed method includes: the registration and evidence of signals, the extraction of informative spectral features, the formation of a RL model with the formalization of the state of the environment, actions and remuneration functions, as well as the mechanism for making diagnostic decisions. Experimental studies on verified data sets (CWRU Bearing Data, MIMII DATASET, DCASE2020 CHALLENGE) demonstrated high efficiency of the method: classification accuracy up to 98.5%, response time 0.5-0.7 seconds at low computing load (36.5% CPU, 509 MB RAM). The results confirm the practical applicability of the method for monitoring the state of equipment in conditions of external noise and non -stationary signals. Promising directions of development include integration with IOT platforms, increasing noise resistance and the introduction of advanced RL algorithms.

**Keywords:** acoustic diagnosis; industrial equipment; reinforcement training; RL-agent; spectral analysis; predictive maintenance; intellectual monitoring systems.

Повышение надежности и безопасности автономно функционирующего промышленного оборудования требует внедрения интеллектуальных систем непрерывного мониторинга [1]. Существующие подходы к акустической диагностике, основанные на методах обучения с учителем, обладают рядом системных ограничений: выраженная зависимость от объемов размеченных данных, низкая адаптивность к динамически изменяющимся условиям эксплуатации и отсутствие механизмов автономного принятия решений в режиме реального времени [2, 3].

Цель данного исследования: разработка, математическое обоснование и экспериментальная верификация метода акустической диагностики, основанного на алгоритмах обучения с подкреплением (Reinforcement Learning, RL), направленного на преодоление указанных ограничений и обеспечивающего высокие показатели точности, адаптивности и ресурсоэффективности.

В основе предложенного метода акустического распознавания неисправностей в работе оборудования лежит синтез спектрального анализа акустических сигналов и RL-парадигмы [4]. Метод включает следующую последовательность этапов:

1. Регистрация и предобработка сигнала: фиксация акустических данных в реальном времени, сегментация, нормализация [5].

2. Извлечение признаков: декомпозиция сигнала на информативные спектральные составляющие с вычислением амплитудного спектра (на основе БПФ), частотного спектра и мел-частотных кепстральных коэффициентов (MFCC) [6].

3. Формирование модели RL: состояние среды (state) формализовано как вектор извлеченных спектральных признаков; действие (action) представляет собой классификацию состояния оборудования; функция вознаграждения (reward) является взвешенной композицией точности классификации и временного штрафа за запаздывание диагностики [7].

4. Принятие решения: выбор оптимального действия (диагностического заключения) на основе стратегии (policy), параметризованной нейронной сетью и оптимизированной для максимизации кумулятивной награды [8].

С использованием разработанного на основе вышеизложенного метода программного обеспечения [9,10] были проведены эксперименты на верифицированных наборах данных (CWRU Bearing Data [9], MIMII Dataset [11], DCASE2020 Challenge [12, 13]). Результаты demonstrated:

- высокую точность классификации: 98.5% для нормального режима работы, 94.2% для состояния с начальными дефектами и 89.7% для критических неисправностей;
- оперативность работы: среднее время отклика системы варьировалось в диапазоне 0.5–0.7 секунды;
- низкую вычислительную нагрузку: средняя загрузка центрального процессора не превышала 36.5% при потреблении оперативной памяти на уровне 509 МБ.

Разработанный метод подтвердил свою эффективность и практическую применимость для мониторинга состояния промышленного оборудования в условиях, характеризующихся наличием внешних шумов и нестационарностью acoustic signals. Ключевыми преимуществами подхода являются адаптивность, обусловленная механизмом обратной связи, и низкие требования к вычислительным ресурсам, что позволяет



рассматривать его для внедрения в составе систем предиктивного обслуживания на базе edge-устройств. Перспективные направления дальнейших исследований включают интеграцию с IoT-платформами, увеличение устойчивости к мультипликативным шумам и имплементацию более совершенных RL-алгоритмов, таких как PPO и A3C.

#### СПИСОК ЛИТЕРАТУРЫ

1. Винограденко А.М., Будко Н.П. Адаптивный контроль технического состояния автономных сложных технических объектов на основе интеллектуальных технологий // T-Comm — Телекоммуникации и Транспорт. 2020. Т. 14. № 1. С. 25–35.
2. Shao S., McAleer S., Yan R., Baldi P. Highly Accurate Machine Fault Diagnosis Using Deep Transfer Learning // IEEE Transactions on Industrial Informatics. 2019. Vol. 15. No. 4. P. 2446–2455.
3. Lu J., et al. Deep learning for diagnosis and classification of faults in industrial rotating machinery // Computers & Industrial Engineering. 2021. Vol. 153. Art. no. 107060.
4. Sutton R.S., Barto A.G. Reinforcement Learning: An Introduction. 2nd ed. Cambridge: MIT Press, 2018. 552 p.
5. Hansen N., Su H., Wang X. Stabilizing Deep Q-Learning with ConvNets and Vision Transformers under Data Augmentation // Advances in Neural Information Processing Systems. 2021. Vol. 34. P. 1–13.
6. Salahul Haq A., Nasrun M., Setianingsih C., Ary Murti M. Speech Recognition Implementation Using MFCC and DTW Algorithm for Home Automation // Proceeding of the Electrical Engineering Computer Science and Informatics. 2020. Vol. 7. P. 78–83.
7. Zhang J., Koppel A., Singh Bedi A., Szepesvari C., Wang M. Variational Policy Gradient Method for Reinforcement Learning with General Utilities // arXiv:2007.02151 [cs.LG]. 2020.
8. Ramaswamy A., Hüllermeier E. Deep Q-Learning: Theoretical Insights from an Asymptotic Analysis // arXiv:2008.10870 [cs.LG]. 2020.
9. Свидетельство о государственной регистрации программы для ЭВМ № 2025619237. Акустическая система диагностики неисправностей промышленного оборудования на основе обучения с подкреплением (АСД-ОП) Правообладатель: Государственное бюджетное образовательное учреждение высшего образования «Нижегородский государственный инженерно-экономический университет» Авторы: Бердникова А.А., Колбанёв М.О., Верзун Н.А., Салиева А.Р. Заявка № 2025617991. Дата поступления 10 апреля 2025 г. Дата государственной регистрации в Реестре программ для ЭВМ 14 апреля 2025 г.
10. Верзун Н. А., Колбанёв М. О., Салиева А. Р. Многоагентный ансамблевый алгоритм акустического распознавания нарушений работоспособности автономного технологического оборудования. // Информационно-управляющие системы, 2025, № 3, С. 14–24. <https://doi.org/10.31799/1684-8853-2025-3-14-24>.
11. Case Western Reserve University Bearing Data Center [Электронный ресурс]. URL: <https://csegroups.case.edu/bearingdatacenter/home> (дата обращения: 10.05.2024).
12. Purohit H., et al. MIMII Dataset: Sound Dataset for Malfunctioning Industrial Machine Investigation and Inspection // arXiv:1909.09347 [eess.AS]. 2019.
13. Koizumi Y., et al. Description and Discussion on DCASE2020 Challenge Task2: Unsupervised Anomalous Sound Detection for Machine Condition Monitoring // DCASE2020 Workshop. 2020.



## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТРАНСПОРТНЫХ СИСТЕМ

УДК 629.122

### ЭВОЛЮЦИЯ СУДОВЫХ ДВИЖИТЕЛЕЙ

Амелаханов Даниил Станиславович, Журавлев Антон Евгеньевич

Государственный университет морского и речного флота имени адмирала С. О. Макарова

Двинская ул., 5/7, Санкт-Петербург, 198035, Россия

e-mails: amelakhanovds@mail.ru, zhuravlevae@gumrf.ru

**Аннотация.** В статье рассматривается эволюция судовых движителей от весельных и парусных судов до современных гребных винтов, водометов и альтернативных установок, а также их влияние на эффективность, маневренность и экологическую устойчивость современного судостроения.

**Ключевые слова:** судовые движители; водный транспорт; эволюция судостроения.

### EVOLUTION OF MARINE PROPULSION SYSTEMS

Amelakhanov Daniil<sup>1</sup>, Zhuravlev Anton<sup>1</sup>

Admiral Makarov State University of Maritime and Inland Shipping

5/7 Dvinskaya str, Saint-Petersburg, 198035, Russia

e-mails: amelakhanovds@mail.ru, zhuravlevae@gumrf.ru

**Abstract.** This article examines the evolution of marine propulsion systems from oars and sailboats to modern propellers, waterjets and alternative propulsion systems, and their impact on the efficiency, maneuverability and sustainability of modern shipbuilding.

**Keywords:** ship propulsion units; water transport; evolution of shipbuilding.

Судоходство исторически эволюционировало от использования парусов и весельных систем к современным высокотехнологичным движителям. В статье Заименко В.К., Балашова М.Г. и Мылимко В.С. представлен обзор основных типов судовых движителей от древнейших — весел и парусов — до современных гребных винтов, колес, крыльчатых и водометных установок. Авторы раскрывают принципы их работы, особенности конструкции и области применения, отмечая преимущества и недостатки каждого вида. Отдельное внимание уделено развитию гребных винтов, которые благодаря простоте, надежности и высокому КПД стали наиболее распространенными в современном судостроении [1].

Мильрат А.В. провел сравнительный анализ судовых движителей. Автор отмечает, что гребной винт обеспечивает высокий КПД (60–80%) и универсальность, но ограничен по глубине эксплуатации; крыльчатый движитель повышает маневренность и применяется на тихоходных судах и подруливающих устройствах, однако имеет сложную конструкцию и КПД 50-60%; водометный движитель обеспечивает отличную маневренность и скорость на мелководье, но на малых скоростях КПД снижен до 35-45%, а конструкция требует высокой точности и стоимости изготовления. Выбор движителя зависит от назначения и условий эксплуатации судна [2].

В работе Паневой А.В. и Цыварева А.А. рассматриваются перспективы применения судовых ветродвижителей, включая паруса-крылья, роторы Флеттнера и воздушные змеи. Авторы отмечают их ключевые преимущества — использование возобновляемой энергии ветра, снижение расхода топлива и выбросов углекислого газа, высокую маневренность и простоту управления, а также ограничения, связанные с зависимостью от ветровых условий, высокой стоимостью установки и применением в основном на вспомогательных движителях. Примеры успешного использования включают грузовые суда, пассажирские паромы и экспериментальные контейнеровозы, где внедрение роторных парусов и кайтов позволило снизить расход топлива на 6–20% [3].

В статье Жукова В.А. и Мильрата А.В. рассматривается использование водометных движителей на судах и кораблях. Авторы анализируют историю их развития, конструктивные особенности осевых, диагональных и осе-диагональных водометов, а также перспективы применения на малотоннажных и скоростных судах. Отмечается, что водометные движители обеспечивают высокую маневренность, безопасность, возможность работы на мелководье и повышенную эффективность на высоких скоростях, хотя на низких скоростях их КПД ниже традиционного гребного винта. Перспективным направлением является конвертация автомобильных высокооборотных двигателей и модернизация их систем охлаждения, смазки, впуска и выпуска для использования в комплексе с водометными движителями [4].

В работе Патиной И.Н., Ефремова В.С. и Родомановой К.С. рассматриваются перспективы применения турбопаруса (ротора Флеттнера) на современных судах. Авторы отмечают его преимущества — высокие тяговые характеристики, простоту управления и обслуживания, возможность автоматизации, снижение нагрузки на главный двигатель и экономию топлива, а также недостатки, связанные с необходимостью энергии на вращение ротора, ограничениями при сильном ветре и зависимостью от наличия ветра. На примере танкера «Maersk Pelican» показано, что использование турбопарусов позволяет сократить годовой расход топлива и выбросы на 8,2% [5].

Современные судовые движители способствуют росту и прогрессу судостроения, обеспечивая повышенную эффективность, маневренность и экономию топлива, при этом выбор конкретного типа зависит от назначения судна, условий эксплуатации и возможностей использования альтернативной энергии. Судостроение исторически развивалось вместе с совершенствованием движителей — от простейших плотов и лодок с веслами до современных высокотехнологичных установок, включая гребные винты, водометы и ветровые системы.

Первые парусные суда появились примерно в 4000 — 3000 лет до нашей эры. Они позволили людям использовать силу ветра для увеличения дальности и скорости плавания, что значительно облегчало перемещение по водным путям. Появление парусов стало важным шагом в развитии мореплавания и судостроения, открывая возможности для дальних торговых и исследовательских экспедиций. С их помощью суда могли преодолевать большие расстояния без постоянного участия гребцов, что повышало эффективность и безопасность плаваний.

В Древней Греции и Риме активно совершенствовались галеры, оснащенные как парусами, так и веслами, что позволяло сочетать использование ветра и силы человека для передвижения. В этот период происходило развитие каркасных конструкций корпусов, которые делали суда более прочными и долговечными. Также совершенствовались механизмы управления движением, включая рулевое устройство и систему расположения гребцов. Эти усовершенствования значительно повышали маневренность и эффективность судов на морских и речных маршрутах.

В Средние века парусные системы претерпели значительные усовершенствования на таких судах, как каравеллы и дромоны. Эти изменения позволяли кораблям использовать ветер более эффективно, что обеспечивало возможность совершать дальние морские экспедиции. Усиленное вооружение и улучшенные парусные конструкции способствовали развитию как торгового, так и военного флота. В результате суда стали более маневренными, надежными и приспособленными к длительным плаваниям.

С началом промышленной революции судостроение претерпело значительные изменения. Паровые двигатели начали заменять часть парусного флота, обеспечивая независимость от ветра и более стабильную скорость движения. Одновременно стали активно использовать гребные винты, которые повышали эффективность преобразования энергии в движение. Внедрение металлических корпусов существенно увеличило прочность судов и продлило их срок службы, сделав их более надежными для дальних и тяжелых рейсов.

В двадцатом веке судостроение продолжило активно развиваться, внедряя новые типы двигателей и движителей. Появились дизельные и газовые турбины, которые обеспечивали более высокую мощность и экономичность по сравнению с паровыми установками. Одновременно начали использовать водометные и крыльчатые движители, повышавшие маневренность и скорость судов, особенно на мелководье и при скоростных рейсах. Эти нововведения также способствовали повышению безопасности и надежности судов в различных условиях плавания.

В современный период судостроение все больше сосредотачивается на разработке и внедрении альтернативных движителей. Особое внимание уделяется турбопарусам, которые используют энергию ветра для движения судов. Появляются гибридные и электрические установки, способные сочетать традиционные двигатели с возобновляемыми источниками энергии. Эти инновации позволяют значительно снижать расход топлива и сокращать выбросы углекислого газа, повышая экологическую эффективность судоходства.

Исторический путь от весел и парусов до гребных винтов, водометов и современных альтернативных движителей показывает, как технический прогресс открывал новые возможности для дальних экспедиций, увеличения скорости и снижения расхода топлива. В современный период особое значение приобретают экологически эффективные и возобновляемые источники энергии, такие как турбопаруса, что позволяет сочетать экономическую выгоду с уменьшением воздействия на окружающую среду.

#### СПИСОК ЛИТЕРАТУРЫ

1. Заименко, В. К. Типы судовых движителей / В. К. Заименко, М. Г. Балашов, В. С. Мылымко // Актуальные вопросы проектирования, постройки и эксплуатации морских судов и сооружений : труды всероссийской научно-практической конференции, Севастополь, 04–05 декабря 2024 года. Севастополь: ФГАОУ ВО «Севастопольский государственный университет», 2024. С. 37–45. EDN PWCUIP.
2. Мильрат, А. В. Сравнительная оценка эффективности судовых движителей / А. В. Мильрат // Транспорт. Горизонты развития : Труды 4-го Международного научно-промышленного форума, Нижний Новгород-Новосибирск-Владивосток-Самара, 23–26 апреля 2024 года. Нижний Новгород: Волжский государственный университет водного транспорта, 2024. С. 40. EDN DHCXWW.
3. Панева, А. В. Перспективы развития технологии движителей / А. В. Панева, А. А. Цыварев // Актуальные вопросы инновационного развития Арктического региона РФ : Сборник материалов IV Всероссийской научно-практической конференции, Северодвинск, 14–30 ноября 2022 года / Министерство науки и высшего образования Российской Федерации, Федеральное государственное образовательное учреждение высшего образования «Северный (Арктический) федеральный университет имени М.В. Ломоносова», 2023. С. 257–261. EDN OTXHV.
4. Жуков, В. А. Водометные движители в судовой энергетике: история и перспективы / В. А. Жуков, А. В. Мильрат // Транспортное дело России. 2022. № 6. С. 34–38. DOI 10.52375/20728689\_2022\_6\_34. EDN PDLSD.
5. Перспектива оснащения турбопарусом современных судов // Неделя науки Санкт-Петербургского государственного морского технического университета. 2022. № 2-2. EDN CWQQU.

УДК 004.056

**ИСПОЛЬЗОВАНИЕ ТЕЛЕМАТИКИ НА ТРАНСПОРТЕ****Богданова Полина Вадимовна**

Государственный университет морского и речного флота имени адмирала С. О. Макарова

Двинская ул., 5/7, Санкт-Петербург, 198035, Россия

e-mail: Emo40@yandex.ru

**Аннотация.** Рассмотрены технологии телематики, в частности, системы мониторинга, исследованы уязвимости телематических систем и основные методы их защиты.

**Ключевые слова:** мониторинг; комплекс технологий; спутниковая навигация; программное обеспечение; уязвимости; угрозы; безопасность.

**USING TELEMATICS IN TRANSPORT****Bogdanova Polina**

Admiral Makarov State University of Maritime and Inland Shipping

5/7 Dvinskaya St., St. Petersburg, 198035, Russia

e-mail: Emo40@yandex.ru

**Abstract.** Telematics technologies are considered, in particular, monitoring systems, vulnerabilities of telematics systems and basic methods of their protection are investigated.

**Keywords:** monitoring; complex of technologies; satellite navigation; software; vulnerabilities; threats; security.

Одним из ключевых средств информатизации стала телематика, которая кардинально поменяла подходы к управлению транспортом и его эксплуатацией. Особую значимость телематические решения приобретают в контексте развития интеллектуальных транспортных систем и перехода к автономному транспорту. Эти технологии позволяют не только повысить эффективность, но и принципиально изменить подходы к системам управления транспортом [1, 2].

Основными возможностями телематики являются мониторинг и отслеживание, которые позволяют получить данные об объектах в реальном времени, а также осуществлять удаленный контроль, анализ и диагностику транспортного средства. Происходит это с помощью интегрируемых GPS- или ГЛОНАСС-трекеров, которые получают данные от спутников и передают их на серверный центр мониторинга. В случае районов без мобильной связи используются спутниковая связь, подвижные точки доступа или коротковолновая радиосвязь. При локальном отсутствии связи данные с телематического оборудования накапливаются в подвижной точке доступа, находящейся на транспортном средстве. Данная точка покидает рабочую зону и собирает информацию с объектов мониторинга, находящихся рядом. После этого, когда транспорт вернется в зону со связью, все данные автоматически попадут на сервер.

Спутниковая система мониторинга, в свою очередь, построена на основе системы спутниковой навигации, оборудования, технологий связи, компьютерной техники и цифровых карт. Основным объектом является бортовой блок, который и определяет скорость, местоположение и другие характеристики транспорта. Сама система строится на основе модульного принципа [3], включающего:

1. Периферийный уровень — состоит из бортовых терминалов, оснащенных GPS/ГЛОНАСС приемниками, акселерометрами и подключаемыми датчиками. Эти устройства используют микропроцессоры с энергоэффективной архитектурой ARM, работающие под управлением реального времени. Современные терминалы поддерживают технологию edge computing, позволяющую выполнять первичную обработку данных непосредственно на устройстве.

2. Транспортный уровень — реализует гибридную схему передачи данных.

3. Облачный уровень — построен на базе распределенных микросервисных архитектур и отвечает за обработку, хранение и анализ непрерывных потоков телематических данных, поступающих от тысяч транспортных средств в режиме реального времени.

Несмотря на все преимущества, внедрение телематических решений в транспортную отрасль сопровождается рядом киберугроз, способных нарушить работу систем мониторинга, управления и связи. Основные риски включают:

1. Подмена GPS- и ГЛОНАСС-данных, манипуляция показаниями датчиков, взлом систем дистанционного управления, вмешательство в работу телематических терминалов [4]. Злоумышленники могут исказить информацию о местоположении, скорости или состоянии транспортного средства, что приводит к авариям или несанкционированному использованию техники.

2. Спуфинг спутниковых сигналов, перехват данных (MITM-атаки), блокирование передачи телеметрии, атаки на сети IoT, используемые для обмена информацией между транспортными средствами и инфраструктурой. Особую опасность представляют атаки на гибридные каналы связи (сотовая, спутниковая, радиосвязь), которые могут привести к потере контроля над автопарком.

3. Заражение бортовых терминалов через уязвимости в прошивках, атаки на облачные серверы обработки данных, вирусы-шифровальщики, блокирующие доступ к телематическим системам. Угрозу также представляют уязвимости в edge-устройствах, выполняющих предварительную обработку данных.

4. Перегрузка облачной инфраструктуры, отвечающей за сбор и анализ данных, что может парализовать работу диспетчерских центров и систем управления транспортом в реальном времени.
5. Установка непроверенных трекеров, датчиков или коммуникационных модулей, которые могут содержать уязвимости или преднамеренно искажать данные.
6. Атаки на системы прогнозирования маршрутов, анализа поведения водителей или автономного управления, включая data poisoning (подмену обучающих данных) и adversarial-атаки, направленные на обман нейросетевых моделей.
7. Устаревшее ПО, где присутствует недостаточная проверка вводимых данных [5].

Для предотвращения или избегания подобных угроз необходимо внедрять многоуровневую систему кибербезопасности.

Защита систем мониторинга и управления требует строгой аутентификации устройств, использования цифровых сертификатов и аппаратных модулей доверенной загрузки (HSM) для бортовых терминалов. Критически важные данные (координаты, показания датчиков) должны передаваться в зашифрованном виде с применением алгоритмов криптографии. Для противодействия спуфингу GPS/ГЛОНАСС следует использовать мультисенсорные системы навигации, включая инерциальные датчики и лидарные технологии, а также применять методы криптографической верификации спутниковых сигналов.

Защита каналов связи должна включать гибридные схемы шифрования (например, комбинацию симметричных и асимметричных алгоритмов), VPN-туннели для передачи данных, а также резервирование каналов связи. В случае использования IoT-сетей необходимо применять стандарты безопасности, такие как TLS 1.3 и защищенные протоколы MQTT. Для предотвращения MITM-атак рекомендуется использовать механизмы взаимной аутентификации устройств и инфраструктуры.

Борьба с вредоносным ПО требует внедрения специализированных антивирусных решений для embedded-систем, регулярного обновления прошивок и контроля целостности ПО. Доступ к USB-портам и другим интерфейсам бортовых терминалов должен быть ограничен, а все внешние носители — проверяться системами sandboxing.

Защита от DDoS-атак подразумевает разворачивание облачных сервисов фильтрации трафика, использование балансировщиков нагрузки и создание избыточной инфраструктуры. Сегментация сетей и применение систем обнаружения аномалий (AI-based IDS) помогут своевременно выявлять атаки.

Для защиты от GPS-спуфинга и MITM-атак следует применять резервные системы навигации, такие как инерциальные датчики, а также использовать криптографические методы защиты данных (например, цифровые подписи и шифрование сигналов). Системы GMDSS должны дублироваться и регулярно тестироваться на устойчивость к кибератакам.

Заражение вирусами через USB-носители и другие внешние устройства можно предотвратить с помощью политики «чистых носителей» и автоматизированных систем проверки подключаемых устройств. Установка специализированных антивирусных решений для промышленных систем (ICS/SCADA) и регулярное обучение экипажа основам кибергигиены помогут снизить риски. В случае ransomware-атак [6] критически важно иметь резервные копии данных и отработанные процедуры восстановления.

Искусственный интеллект и системы автоматизированного принятия решений [7] должны разрабатываться с учетом рисков атак на данные (data poisoning) и эксплуатации уязвимостей алгоритмов. Тестирование на устойчивость к adversarial-атакам и постоянный мониторинг работы моделей помогут снизить потенциальные угрозы [8].

## СПИСОК ЛИТЕРАТУРЫ

1. Нырков А.П. Методы повышения эффективности работы портов в рамках международных транспортных коридоров / А. П. Нырков, Т. Дмитриева, С. С. Соколов // Речной транспорт (XXI век). № 6 (42), 2009. С. 75-77.
2. Нырков А.А. Автоматизация информационного обеспечения деятельности исследовательской проблемной лаборатории / Нырков А.А., Нырков А.П. // Сб. науч. тр. «Управление транспортными системами». СПб.: СПГУВК, 1997. С. 98-99.
3. Малых Д. А. Использование модульного принципа построения для проектирования различных вариантов исполнения универсальной космической платформы, 2023 [Электронный ресурс]. URL: <https://mai.ru/upload/iblock/50c/xqaf7umes6xls456e9z9kgjvd9ffsf24/6-Malykh.pdf?ysclid=mdik3j15pf540456551> (дата обращения 17.07.2025).
4. Матвеев А. А., Кузнецов В. Н., Гаскаров В. Д. Обзор технических средств и методов спутниковой навигации судов, 2016 [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/obzor-tehnicheskikh-sredstv-i-metodov-sputnikovoy-navigatsii-sudov> (дата обращения 18.07.2025).
5. Нырков А.П. Обеспечение безопасности объектов информатизации транспортной отрасли / под ред. А. П. Ныркова. / А. П. Нырков, А. А. Нырков, С. С. Соколов, А. А. Шнуренко // СПб.: Изд-во Политехн. ун-та, 2015. 544 с.
6. Назаров А. В., Марьенков А. Н., Калиев А. Б. Выявление поведенческих признаков работы вируса-шифровальщика на основе анализа изменений значений параметров компьютерной системы // Прикаспийский журнал: управление и высокие технологии. 2018. №1 (41). URL: <https://cyberleninka.ru/article/n/vyyavlenie-povedencheskikh-priznakov-raboty-virusa-shifrovalshchika-na-osnove-analiza-izmeneniy-znacheniy-parametrov-kompyuternoy> (дата обращения: 20.07.2025).
7. Арбузов А.М. Применение алгоритмов машинного обучения в обеспечении безопасности сетевой инфраструктуры IoT-систем на водном транспорте / А. М. Арбузов, А. П. Нырков, А. Н. Терехов, И. В. Ли, Д. А. Деменив // Проблемы информационной безопасности. Компьютерные системы. №2. 2025. С. 131-142.
8. Нырков А.П. Оптимизация процесса тестирования на проникновение в АСУ технологическими процессами с использованием алгоритмов машинного обучения / А. П. Нырков, Е. С. Юмашева, А. В. Кириков // Вестник государственного университета морского и речного флота им. адмирала С.О. Макарова. Т. 16. № 3. 2024. С. 456-466.

УДК 004.942

**АЛГОРИТМ РАСХОЖДЕНИЯ ВСТРЕЧНЫХ СУДОВ НА ОСНОВЕ  
МЕТОДА ПОТЕНЦИАЛЬНЫХ ПОЛЕЙ****Данилин Герман Владиславович, Худайназаров Юрий Кахрамонович, Соколов Сергей Сергеевич**

Государственный университет морского и речного флота имени адмирала С. О. Макарова

Двинская ул., 5/7, Санкт-Петербург, 198035, Россия

e-mails: t.101@mail.ru, yu-78@yandex.ru, sokolovss@gumrf.ru

**Аннотация.** Развитые страны мира сегодня стремятся освоить технологии беспилотного транспорта. Российские исследователи, руководствуясь такими инициативами как «Маринет» и «Стратегия развития беспилотной авиации до 2030 года», также ведут работы в данном направлении. В вопросе освоения беспилотных систем одной из ключевых остается задача разработки надёжных и безопасных систем управления, способствующих снижению аварийности относительно пилотируемого транспорта. Данная работа является частью исследования, посвященного созданию методики вычисления параметров траекторного управления, обеспечивающих заданную вероятность успешного безопасного маневра.

**Ключевые слова:** водный транспорт; безэкипажное судоходство; обход препятствий; метод потенциальных полей; автономное судно.

**ALGORITHM FOR DISTANCE MANAGEMENT OF MEETING VESSELS BASED  
ON THE METHOD OF POTENTIAL FIELDS****Danilin German, Khudainazarov Yuri, Sokolov Sergey**

Admiral Makarov State University of Maritime and Inland Shipping

5/7 Dvinskaya St., St. Petersburg, 198035, Russia

e-mails: t.101@mail.ru, yu-78@yandex.ru, sokolovss@gumrf.ru

**Abstract.** Today, developed countries around the world are striving to master the technology of unmanned transport. Russian researchers, guided by initiatives such as «Marinet» and the «Strategy for the Development of Unmanned Aviation until 2030», are also working in this direction. In the field of unmanned systems, one of the key challenges remains the development of reliable and safe control systems that can reduce accidents compared to manned vehicles. This work is part of a research project aimed at creating a methodology for calculating trajectory control parameters that ensure a specified probability of successful maneuvering.

**Keywords:** water transport; unmanned navigation; obstacle avoidance; potential field method; and autonomous vessels.

Развитые страны мира сегодня стремятся освоить технологии беспилотного транспорта. Российские исследователи, руководствуясь такими инициативами как «Маринет» и «Стратегия развития беспилотной авиации до 2030 года», также ведут работы в данном направлении. В вопросе освоения беспилотных систем одной из ключевых остается задача разработки надёжных и безопасных систем управления, способствующих снижению аварийности относительно пилотируемого транспорта. Данная работа является частью исследования, посвященного созданию методики вычисления параметров траекторного управления, обеспечивающих заданную вероятность успешного маневра.

Ранее в работах [1, 2] изучались математические модели движения судна, проводились эксперименты по расчету параметров движения судна, а также был рассмотрен алгоритм уклонения автономного судна от препятствий [3], основанный на использовании метода потенциальных полей [4-6].

В данной работе была проведена серия экспериментов, посвященных изучению поведения алгоритма на примере манёвра расхождения двух встречнодвижущихся судов.

В ходе экспериментов было отмечено, что исходный алгоритм обхода препятствий обладает погрешностью, проявляющейся при установке значений курса судов отличными от 0°.

Прямолинейное движение судов оказалось возможным при изначальном курсе 0° или 180°, следовательно, прямолинейность движения зависима от погрешности, вносимой перерасчетом векторов скоростей судов, осуществляемых на каждом шаге алгоритма.

Эксперименты показали, что при строгом следовании судов обратными курсами по одной линии, параллельной оси абсцисс, алгоритм заклинивается и не может рассчитать маршрут движения.

При перекрестном движении судов возникла аналогичная проблема: при схождении судов на дистанции учета потенциалов алгоритм оказался не в состоянии построить маршрут движения судов.

В исходный алгоритм было добавлено дополнительное проверочное условие, учитывающее требования МППСС-72, предписывающее правила расчета векторов скоростей судов в подобной ситуации. Указанное дополнение к алгоритму помогло решить проблему ухода от лобового столкновения судов.

На следующем этапе была успешно проведена проверка возможности обхода статичного препятствия судами, совершающими расхождение при встречном следовании обратными курсами. Наилучшим образом алгоритм в исходном виде проявляет себя тогда, когда в рабочей области оказывается небольшое количество препятствий и встречно движущихся судов, находящихся на значительном удалении друг от друга. Усовершенствованный алгоритм обхода препятствий не избавлен от погрешности, связанной с механизмом расчета векторов скоростей судов, однако, учитывает ранее не учитываемые сценарии движения судов.

Первый этап работы был посвящен проведению серии экспериментов, изучающей поведение алгоритма обхода препятствий, основанного на методе потенциальных полей, в случае осуществления манёвра расхождения двух встречно движущихся судов. В результате экспериментов было сделано предположение о наличии у алгоритма погрешности, зависящей от особенностей осуществления расчетов параметров, входящих в его состав. В процессе экспериментальной проверки выдвинутого предположения, была выявлена неспособность алгоритма строить маршрут движения судов при некоторых сценариях их движения. В ходе второго этапа работы было выработано решение по усовершенствованию алгоритма обхода препятствий, учитывающее данные сценарии. В результате дальнейших экспериментов было установлено, что с учетом проведенной доработки алгоритм стал способен строить маршруты расхождения судов как в случае отсутствия на маршруте следования статических препятствий, так и при их наличии.

Направлением дальнейшего развития данного исследования может стать проработка поведения алгоритма при других сценариях движения судов и расположения препятствий. Кроме того, усовершенствованный алгоритм может служить основой для разработки методики вычисления параметров траекторного управления, обеспечивающих заданную вероятность успешного маневра.

#### СПИСОК ЛИТЕРАТУРЫ

1. Данилин, Г. В. Исследование математических моделей движения судна и технологий безэкипажного судовождения / Г. В. Данилин, С. С. Соколов // Сборник научных статей национальной научно-практической конференции профессорско-преподавательского состава «ГУМРФ им. адм. С. О. Макарова», Том 1. СПб.: Изд-во ГУМРФ им. адм. С. О. Макарова, 2022. С. 72-78.
2. Данилин, Г. В. Расчет параметров движения безэкипажного судна в программной среде Maple 1 / Г. В. Данилин, С. С. Соколов // Региональная информатика и информационная безопасность. Сборник трудов. Вып. 12. СПб.: СПОИСУ, 2023. С. 214-216.
3. Данилин, Г.В. Модель движения автономного судна, учитывающая условия движения в стесненной акватории / Г.В. Данилин, С.С. Соколов, Ю.Ф. Каторин // Известия Тульского государственного университета. Технические науки. 2024. № 5. С. 208-213.
4. Кабиняков, М. Ю. Метод предотвращения столкновений для агентов мультироботизированных систем на основе машинного обучения и метода потенциальных полей / М. Ю. Кабиняков // Перспективы науки. 2021. № 8(143). С. 22-29.
5. Nyrkov, A.P. Development of underwater robotics / A. P. Nyrkov, A. A. Zhilenkov, V. V. Korotkov, S. S. Sokolov, S. G. Chernyi // Journal of Physics: Conference Series, Volume 803, Issue 1, 2017. № 012108.
6. Пшихопов, В.Х. Групповое управление движением мобильных роботов в неопределенной среде с использованием неустойчивых режимов / В.Х. Пшихопов, М.Ю. Медведев // Труды СПИИРАН. 2018. № 5(60). С. 39-63.

УДК 004.08

### ОЦЕНКА ПРОИЗВОДИТЕЛЬНОСТИ АВТОМОБИЛЬНЫХ LIDAR И РАДАРОВ В УСЛОВИЯХ ПЛОХОЙ ВИДИМОСТИ

Вавкина Елена Александровна

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевики пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mail: vavkina.e.a@fsin.gov.ru

**Аннотация.** Исследуется влияние тумана, снега и плохой видимости на работу LiDAR и радаров в автономных автомобилях. Рассматриваются проблемы снижения точности и дальности обнаружения, а также методы сенсорной интеграции и обработки данных для повышения надежности систем в сложных погодных условиях.

**Ключевые слова:** автономное вождение; автономные транспортные средства; системы помощи водителю (ADAS); lidar; радар; туман; снегопад; осадки; точность срабатываний.

### EVALUATION OF THE PERFORMANCE OF AUTOMOTIVE LIDAR AND RADAR SYSTEMS IN BAD VISIBILITY CONDITIONS

Vavkina Elena

The Bonch-Bruевич Saint Petersburg State University of Telecommunications  
22 Bolshhevikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mail: vavkina.e.a@fsin.gov.ru

**Abstract.** The impact of fog, snow, and poor visibility on the operation of LiDAR and radars in autonomous vehicles is being investigated. The problems of reduced accuracy and detection range are being addressed, as well as methods for sensor integration and data processing to improve the reliability of systems in challenging weather conditions.

**Keywords:** autonomous driving; autonomous vehicles; driver assistance systems (ADAS); lidar; radar; fog; snowfall; precipitation; accuracy of detections.

В современном автомобильном мире сенсорные системы, такие как LiDAR и радары, играют ключевую роль в обеспечении безопасности и автономности транспортных средств. Эти устройства позволяют автомобилям с искусственным интеллектом воспринимать окружающую среду, распознавать препятствия и принимать решения в режиме реального времени. Однако эффективность работы таких датчиков значительно зависит от погодных условий, особенно в условиях тумана, обильного снегопада и плохой видимости [1].

LiDAR, основанный на принципе лазерного сканирования, создает детальную трёхмерную карту окружающего пространства. Его высокая точность и разрешение делают его незаменимым для автономных

систем. Однако лазерные лучи, используемые LiDAR, сильно рассеиваются в присутствии атмосферных частиц, таких как капли воды в тумане или снежинки. Это приводит к снижению дальности обнаружения объектов, появлению шумов и ложных сигналов, что ухудшает качество восприятия окружающей среды. В условиях густого тумана или плотного снегопада эффективность LiDAR может значительно снижаться, вплоть до полной потери возможности обнаружения дальних объектов [2].

Радары, в отличие от LiDAR, используют радиоволны, которые обладают большей проникающей способностью через атмосферные осадки. Это делает радарные системы более устойчивыми к туманам и легким осадкам. Тем не менее, сильный снегопад, град или интенсивный дождь также могут оказывать негативное влияние на работу радаров, вызывая искажения сигналов, снижение точности измерений и появление ложных отражений. Несмотря на это, радары в целом считаются более надежными в сложных погодных условиях по сравнению с LiDAR.

Зимние погодные условия вводят в работу систем автономного вождения ряд помех: накопление снега на дорожных знаках затрудняет их распознавание; снегопад создаёт значительный шум в данных, получаемых от сенсоров (например, LiDAR и камеры); снеговой покров и грязь маскируют дорожную разметку; загрязнение датчиков на самом автомобиле также ухудшает качество данных [3].

Однако многие из этих проблем потенциально решаемы. Для снижения шума, вносимого снегопадом на изображениях с камер, могут быть применены существующие алгоритмы, аналогичные тем, которые используются для подавления теплового шума в условиях низкой освещенности. Данный подход демонстрирует возможность адаптации уже известных методик обработки данных к условиям зимнего вождения.

Принцип работы лидара существенно отличается от функционирования традиционных камер. Лидар является активным датчиком, который излучает лазерные импульсы и измеряет время их отражения от объектов, что позволяет точно определять расстояние до них. Обработка множества отражённых импульсов формирует трёхмерное облако точек, обеспечивая детальное пространственное моделирование окружающей среды. Современные лидары ведущих производителей, таких как Velodyne, способны генерировать сотни тысяч, а иногда и миллионы точек в секунду, что делает их наиболее точными и многофункциональными сенсорами, превосходящими по возможностям камеры и радары [4].

В индустрии автономного вождения сложился консенсус, что лидары являются ключевыми элементами для создания безопасных и надёжных беспилотных систем, за исключением позиции компании Tesla, которая традиционно отказывается от использования данной технологии.

Учитывая значимость лидаров, одной из приоритетных задач является фильтрация помех, вызванных снегом, в трёхмерных облаках точек. Обычно это реализуется путём анализа плотности распределения точек, однако также применяются более сложные методы, позволяющие оценивать свойства непрозрачной среды и исключать сигналы, поступающие из неё. Фильтрация сигнала относится к этапу первичной обработки данных, после чего следует семантический анализ, направленный на извлечение смысловой информации. [5]

Именно решение этой задачи является центральным в конкурсе Ice Vision. Организаторы мероприятия, проводившие исследования на реальных российских дорогах, сформировали обширный датасет, включающий более 20 тысяч кадров. Для каждого временного момента доступны данные с двух камер, лидаров, трёх GPS-приёмников и инерциального блока, что обеспечивает комплексный набор информации для разработки и тестирования алгоритмов в условиях зимнего вождения.

Многочисленные эксперименты и исследования, проведенные в последние годы, подтверждают эти наблюдения. В лабораторных и полевых условиях тестировались различные модели LiDAR и радаров при имитации тумана, снега и дождя. Результаты показали, что при ухудшении видимости дальность и точность обнаружения объектов снижаются, а количество ложных срабатываний возрастает. Однако современные системы компенсируют эти недостатки за счет использования сенсорной интеграции — объединения данных от LiDAR, радаров и камер. Такой подход позволяет повысить общую надежность восприятия, комбинируя сильные стороны каждого типа датчиков и минимизируя влияние погодных помех. [6]

Выводы из проведенных исследований однозначны: погодные условия существенно влияют на эффективность работы автомобильных сенсоров. LiDAR наиболее уязвим к туману и снегу, тогда как радары демонстрируют большую устойчивость, но тоже не застрахованы от ухудшения качества данных. Для обеспечения надежной и безопасной работы автономных систем необходимо использовать комплексные решения с интеграцией нескольких видов сенсоров и продвинутыми алгоритмами обработки сигналов. Только такой подход способен гарантировать высокую точность восприятия окружающей среды в разнообразных и сложных дорожных условиях.

В Российской Федерации особенности климата создают особенно сложные условия для работы лидаров и радаров в системах автономного вождения. Длительная зима с постоянными снегопадами, короткое лето и продолжительные периоды осени и весны с гололёдом и обильными осадками значительно осложняют восприятие окружающей среды. Частые утренние туманы дополнительно снижают качество данных с сенсоров. В таких неблагоприятных погодных условиях актуальность разработки и совершенствования методов фильтрации, сенсорной интеграции и алгоритмов обработки данных становится особенно высокой, что необходимо для обеспечения безопасности и надёжности беспилотных систем в России [7].

Актуальность исследования и разработки методов повышения надёжности работы лидаров и радаров в условиях сложных погодных факторов, характерных для России, крайне высока. Это ставит задачу комплексной



проработки алгоритмов фильтрации, адаптации сенсоров и интеграции данных для обеспечения стабильного и точного восприятия окружающей среды [8].

В России и за рубежом ведутся активные разработки в этой области. Например, научно-исследовательские институты, специализирующиеся на робототехнике и автономных системах, совместно с промышленными компаниями проводят испытания и совершенствуют алгоритмы обработки сигналов для повышения устойчивости сенсоров к снегу, туману и дождю и т.д. Среди заметных инициатив — программы тестирования автономных транспортных средств в зимних условиях, направленные на сбор обширных датасетов и разработку специализированных методов обработки данных. Эти усилия способствуют созданию более надёжных технологий, способных эффективно работать в сложных климатических зонах, таких как Российская Федерация, что является ключевым фактором для массового внедрения беспилотных систем на отечественных дорогах.

#### СПИСОК ЛИТЕРАТУРЫ

1. Павловский В. Е. Эвристический алгоритм обнаружения изолированных препятствий мобильным роботом по дальномерным данным // Искусственный интеллект и принятие решений. 2016. № 4. С. 93–105.
2. Kashevnik, A., Ponomarev A., Krasov A. Human-Computer Threats Classification in Intelligent Transportation // Conference of Open Innovations Association, FRUCT. 2020. № 26. P. 151-157.
3. Постолит А.В. Перспективы применения искусственного интеллекта и компьютерного зрения в транспортных системах и подключенных автомобилях // Мир транспорта. 2021. № 19(1). С. 74-90.
4. Tesla тестирует новую систему, которая сделает машины компании полностью автономными // Naked Science: сетевое издание. URL: <https://naked-science.ru/article/hi-tech/full-self-driving-tesla> (дата обращения: 16.08.2025).
5. Попова, М. Л. Перспективы развития автономного транспорта // Молодой ученый. 2021. № 5 (347). С. 11-12.
6. Билятинов К.З., Красов А.В., Меньяло В.В. Исследование систем и анализ результатов испытаний. Санкт-Петербург : Центр научно-информационных технологий «Астерион», 2019. 362 с.
7. Технические аспекты управления с использованием сети Интернет : Монография / А. А. Алейников, К. З. Билятинов, А. В. Красов [и др.]. Санкт-Петербург : Центр научно-информационных технологий «Астерион», 2016. 305 с.
8. Силенко А.Н. Использование искусственного интеллекта в сфере автомобилестроения // Международный журнал прикладных наук и технологий «INTEGRAL». 2024. №1.

УДК 621.391

#### МЕТОДИКА ОЦЕНКИ ДОСТУПНОСТИ СИСТЕМЫ КОРПОРАТИВНОЙ СВЯЗИ СРЕДСТВАМ РАДИОКОНТРОЛЯ И ТЕХНИЧЕСКОГО КОМПЬЮТЕРНОГО КОНТРОЛЯ

Ефанов Антон Сергеевич<sup>1</sup>, Иванов Сергей Александрович<sup>2</sup>

<sup>1</sup> Военная академия связи им. Маршала Советского Союза С. М. Буденного  
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

<sup>2</sup> Государственный университет морского и речного флота имени адмирала С. О. Макарова  
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия  
e-mails: t\_o\_x\_@list.ru, sa-ivanov@inbox.ru

**Аннотация.** Предлагается методика оценки доступности системы корпоративной связи средствам радиоконтроля и технического компьютерного контроля для контроля и управления параметрами ее функционирования. Приведены основные этапы методики.

**Ключевые слова:** доступность; вероятность; система корпоративной связи.

#### METHODOLOGY FOR ASSESSING THE ACCESSIBILITY OF A CORPORATE COMMUNICATION SYSTEM TO RADIO CONTROL AND TECHNICAL COMPUTER CONTROL

Efanov Anton<sup>1</sup>, Ivanov Sergey<sup>2</sup>

<sup>1</sup> The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonn  
3 Tikhoretsky Av, St. Petersburg, 194064, Russia

<sup>2</sup> Admiral Makarov State University of Maritime and Inland Shipping  
5/7 Dvinskaya St., St. Petersburg, 198035, Russia  
e-mails: t\_o\_x\_@list.ru, sa-ivanov@inbox.ru

**Abstract.** A methodology for assessing the availability of a corporate communications system to radio monitoring and technical computer control is proposed for monitoring and managing its operating parameters. The main stages of the methodology are presented.

**Keywords:** availability; probability; corporate communication system.

Контроль за функционированием современных корпоративных систем связи является одной из важнейших задач организации связи в этих системах. Существующие тенденции по обеспечению корпоративных систем связи техникой связи различных технологий (аналоговых и цифровых) требуют новых подходов к оценке их функционирования [1, 2]. Зачастую эти средства применяются совместно, бессистемно и без учета их особенностей. Встает закономерный вопрос о рациональных местах размещения средств радиоконтроля и средств технического компьютерного контроля. Кроме того, повышение экологических норм требует соблюдения функционирования излучающих средств в пределах заданных параметров для исключения влияния на окружающую природную среду, что также является важной задачей для радиоконтроля.

Данная методика позволяет учесть как традиционные (аналоговые) средства связи, так и современные цифровые средства радиосвязи (и другие цифровые средства связи), имеющие возможность работы через сеть связи общего пользования.

Методика оценки вероятности электромагнитной доступности включает следующие этапы: расчёт средней мощности сигнала на входе радиоприёмного устройства (РПУ); расчёт средней мощности шума на входе РПУ; вычисление среднего отношения сигнал/шум; вычисление  $\sigma_z$  — среднеквадратического отклонения превышения уровня сигнала над уровнем шума от его среднего значения; определение  $Z_{тр}$  — требуемого превышения мощности сигнала над мощностью шума; вычисление  $u$  — аргумента интеграла вероятности (функции Лапласа) [3].

При этом уровень сигнала на входе приемника поста радиоконтроля определяется по уравнению радиолинии [4, 5]. Данное уравнение позволяет учесть такие важные параметры как: угол между главным лепестком диаграммы направленности антенны радиоэлектронного средства и лучом на пост радиоконтроля; угол между главным лепестком диаграммы направленности антенны радиоэлектронного средства и лучом на источник радиоизлучения; длина волны излучаемых радиосигналов; расстояние между радиоэлектронным средством и источником радиоизлучения; диаметр антенного зеркала в метрах; коэффициент полезного действия фидеров излучающих и приемных антенн; мощность, подводимую к фидеру источником радиоизлучения. Все эти параметры наиболее полно учитывают условия распространения радиоволн (для земной волны) в пространстве.

Данная методика хорошо себя зарекомендовала в ходе апробаций, программно реализована. Она широко применяется для расчета зон покрытия излучающих средств связи, для расчета дальности связи с различными наземными и воздушными робототехническими средствами.

На данный момент времени утвержденных методик вероятности доступности системы корпоративной связи различного уровня техническому компьютерному контролю нет. Это связано с трудностью интерпретации процессов, происходящих в информационно-телекоммуникационной сети связи общего пользования.

Для методики оценки доступности техническому компьютерному контролю предлагаются следующие этапы: сеть связи моделируется графом сети, вершинами и ребрами которого являются узлы и линии связи; вершины графа представляют собой узлы связи, а ребра — совокупность линий связи (линий передачи), которые соединяют вершины графа между собой; всем элементам графа (вершинам и ребрам) присваивают весовой коэффициент, представляющий собой коэффициент готовности узла или линии связи при расчете показателей надежности сети связи (при расчете показателей живучести весовыми коэффициентами являются коэффициенты оперативной готовности узлов и линий связи).

На построенном графе сети связи выделяют два полюса (две вершины — «исток» и «сток»), которые отмечают выбранное направление связи. Метод расчетной оценки связности между элементами графа с помощью перебора простых цепей заключается в том, что для выбранных полюсов графа сети, в соответствии с алгоритмом установления связи, отмечаются все цепи (или пути), по которым может быть установлено соединение.

Под событием связности понимают такое событие, когда между «исток» и «сток» в работоспособном состоянии существует хотя бы одна простая цепь. Если между полюсами сети в работоспособном состоянии нет ни одной простой цепи, то в двухполюсной сети наступает событие несвязности. Под «простой цепью» понимают последовательность ребер и вершин графа без петель и параллелей, замыкающую полюсы (выбранные вершины) между собой.

Далее на графе сети выделяют все простые цепи между выделенной парой полюсов (узлов). При заданных коэффициентах готовности (или оперативной готовности) для всех элементов графа связность двухполюсной сети между выделенными узлами рассчитывается методом объединения простых цепей с учетом эффекта поглощения.

В соответствии с [6] вероятность связности (связность) направления электросвязи — вероятность того, что на заданном направлении электросвязи существует хотя бы один путь, по которому возможна передача информации с требуемыми качеством и объемом. Функционирование сетей электросвязи, входящих в состав сети связи общего пользования, в условиях воздействия дестабилизирующих факторов физического или технологического характера определяется свойством сети, называемым устойчивостью.

Показатели надежности сети связи (вероятность связности между любыми вершинами случайного графа сети) определяют методом перебора простых цепей. Связностью  $n$ -го пути из перечня всех цепей называется совместная вероятность исправного состояния всех ребер и вершин, образующих эту цепь. Вероятность связности  $n$  от  $k$  — это вероятность исправного состояния хотя бы одной цепи из всех возможных цепей или (при ограничении числа транзитных участков) хотя бы одной цепи с допустимым рангом.

Коэффициент соответствия представляет собой число, показывающее отношение количества узлов, через которые проходит информация от наибольшего количества корреспондентов (информационных направлений), к общему числу узлов. Закономерность распределения данного коэффициента для сетей связи различного ранга (в зависимости от количества узлов) требует дополнительных исследований.

Таким образом, вероятность связности центров техническому компьютерному контролю с узлами связи (вершинами графа), ведущими обмен в сети связи общего пользования для системы корпоративной связи

можно интерпретировать как вероятность доступности системы корпоративной связи с некоторым коэффициентом соответствия.

Итоговую вероятность доступности системы корпоративной связи средствами радиоконтроля и технического компьютерного контроля вычисляют как вероятность совместных событий. Данные события являются совместными так как появление одного из них не исключает появления другого.

Таким образом, данная методика позволяет оценить доступность корпоративной системы связи не только традиционным средствам радиоконтроля, но и перспективным средствам технического компьютерного контроля.

Ее применение возможно в корпоративных системах связи для самоконтроля ее функционирования и управления параметрами средств связи, различными органами экологического контроля в целях соблюдения экологических норм (в части, касающейся электромагнитного излучения) для определенных территорий (заповедников, природных парков, особых охраняемых зон и др.), старшим органом контроля за соблюдением правил ведения переговоров и соблюдения режимов работы излучающих радиосредств.

#### СПИСОК ЛИТЕРАТУРЫ

1. Collection of reports of the conference «Special mobile radio communications» [Electronic resource]. URL: <https://e-edition.ru/katalog/spets-svyaz-17/files/assets/basic-html/page80.html> (date of access: 02.05.2025).
2. Zhilin, M. A. Modern views of the US Department of Defense on the use of electromagnetic radiation for military purposes / M. A. Zhilin // Foreign Military Review. 2022. № 8/2022. P. 30-36. EDN THBRXC. Text: direct.
3. Sevidov V. V., Dvornikov S. S., Bestugin A. R., Dvornikov S. V., Kirshina I. A. Evaluation of electromagnetic availability of radio emission sources starlink gss / High-tech technologies in space research of the earth. 2023/ № 4/2023. P. 26-37. EDN ООО «Publishing House Media Publisher».
4. Mishalkin V. A., Sosunov V. B., Filippov V. V. Fields and waves in the problems of intelligence protection and electronic protection of communication systems: Textbook. St. Petersburg: VAS, 1993. 322.
5. Efanov, V. I. Electromagnetic compatibility of radio-electronic means and systems. Tutorial / V. I. Efanov, A. A. Tikhomirov // Electromagnetic compatibility of radio-electronic means and systems. Tutorial Tomsk: Tomsk State University of Control Systems and Radioelectronics, 2012. P. 17-22. EDN IHEFLO. Text: direct.
6. GOST R 53111—2008. Stability of operation of the public communications network. Requirements and testing methods.

УДК 004.05

#### МАШИННОЕ ЗРЕНИЕ В АВТОНОМНЫХ ТРАНСПОРТНЫХ СИСТЕМАХ: УГРОЗЫ И АРХИТЕКТУРЫ ДОВЕРИЯ

Изотов Даниил Юрьевич, Яровой Роберт Владимирович

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: daniil.izotov.1999@mail.ru, Nadzar@yandex.ru

**Аннотация.** В тезисе представлены типы воздействий на систему восприятия, включая физические и цифровые атаки, ошибки интерпретации и архитектурные ограничения. Представлены методы верификации, основанные на мультисенсорной интеграции, цифровых двойниках, самоконтроле и обратной связи.

**Ключевые слова:** автономный транспорт; машинное зрение; визуальное восприятие; цифровой двойник; мультисенсорная интеграция; самоконтроль; доверенный ИИ.

#### MACHINE VISION IN AUTONOMOUS VEHICLE SYSTEMS THREAT AND TRUST ARCHITECTURES

Izotov Daniil, Yarovoy Robert

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: daniil.izotov.1999@mail.ru, Nadzar@yandex.ru

**Abstract.** The thesis presents types of influences on the perception system, including physical and digital attacks, interpretation errors and architectural limitations. Verification methods based on multisensory integration, digital twins, self-monitoring and feedback are presented.

**Keywords:** autonomous transport; machine vision; visual perception; digital twin; multisensory integration; self-monitoring; trusted AI.

Визуальное восприятие является критическим модулем в архитектуре автономного транспорта, определяя поведение системы в реальном времени. Ошибки в интерпретации визуальных данных могут привести к недопустимым последствиям, поскольку именно эти данные инициируют управленческие действия: торможение, перестроение, реакцию на препятствия [1].

Источники искажений делятся на четыре категории: внешние физические (блики, загрязнение, засветка), преднамеренные (лазеры, наклейки, ложные объекты), внутренние архитектурные (инвариантность, переобучение, потеря контекста), а также климатические (туман, дождь, тени, свет). Даже минимальные искажения способны вызвать ложную интерпретацию сцены — от пропуска объекта до неправильной классификации [2].

Нейросетевые архитектуры обладают уязвимостями: сверточные сети теряют глобальный контекст, трансформеры требуют сложной регуляризации. Ошибки возникают на всех этапах пайплайна: в детекции, классификации, семантической сегментации [3].

Для снижения рисков требуется верификация восприятия. Эффективным методом выступает мультисенсорная интеграция: сопоставление визуальных данных с показаниями лидаров, радаров и других сенсоров, что позволяет выявлять рассогласования между источниками [4].

Моделирование с использованием цифровых двойников (CARLA, AirSim) позволяет воспроизводить редкие и опасные сценарии: искажения, препятствия, шумы.

В архитектуру perception-стека внедряются модули самоконтроля: они отслеживают внутренние распределения признаков, оценивают метрики доверия и инициализируют переключение на резервные режимы при возникновении сбоев.

Безопасность восприятия требует не изолированной настройки алгоритмов, а системного проектирования — от сенсоров до архитектур доверия. Только комплексная модель с самооценкой, проверкой и адаптацией позволяет создавать транспортные системы, устойчивые к внешним и внутренним сбоям.

#### СПИСОК ЛИТЕРАТУРЫ

1. Синевский Р.М., Ксантиниди К.Х. Перспективы использования автопилотируемых систем // Пространство колес 1520: проблемы, потенциал, перспективы. Сборник трудов Межвузовской студенческой научно-практической конференции с международным участием. Москва, 2024. С. 98-103.
2. Рылов Я.А. Вектор развития автопилотируемых систем для повышения безопасности дорожного движения // Перспективные направления развития автотранспортного комплекса. Сборник статей XVIII Международной научно-практической конференции. Пенза, 2024. С. 120-124.
3. Яровой Р.В., Парашук И.Б. Взаимосвязь машинного зрения и информационной безопасности // Информационная безопасность регионов России (ИБРР-2023). XIII Санкт-Петербургская межрегиональная конференция. Материалы конференции. СПб, 2023. С. 178-180.
4. Кривоногова Е.В., Рябов Г.А., Яровой Р.В. Использование нейросети для интеллектуального анализа изображения // Тенденции развития науки и образования. 2023. № 100-5. С. 40-42.

УДК 004.89: 656.078

#### ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ — КЛЮЧЕВОЙ ЭЛЕМЕНТ ОБЕСПЕЧЕНИЯ ЖИЗНЕСПОСОБНОСТИ ЦЕПЕЙ ПОСТАВОК

Искандеров Юрий Марсович

СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия

e-mail: iskanderov.y@ias.spb.su

**Аннотация.** В докладе дано представление об информационной безопасности как ключевом элементе обеспечения жизнеспособности цепей поставок. Отмечена многократно возрастающая роль безопасности и защищенности задействованных в цепях поставок информационно-телекоммуникационных систем на протяжении всего их жизненного цикла. Показана необходимость определения и формирования единой политики информационной безопасности цепей поставок. Для реализации указанной политики предложена релевантная интеллектуальная система управления информационной безопасностью.

**Ключевые слова:** информационная безопасность; жизнеспособность; цепи поставок; единая политика информационной безопасности; интеллектуальная система; управление.

#### INFORMATION SECURITY IS A KEY ELEMENT IN ENSURING THE VIABILITY OF SUPPLY CHAINS

Iskanderov Yuriy

St. Petersburg Federal Research Center of the Russian Academy of Sciences

39 14th Line VO, St. Petersburg, 199178, Russia

e-mail: iskanderov.y@ias.spb.su

**Abstract.** The report provides an insight into information security as a key element in ensuring the viability of supply chains. The increasing role of security and security of information and telecommunication systems involved in supply chains throughout their entire life cycle is noted. The necessity of defining and forming a unified information security policy for supply chains is shown. A relevant intelligent information security management system has been proposed to implement this policy.

**Keywords:** information security; viability; supply chain; unified information security policy; intelligent system; management.

В современном турбулентном мире важнейшими факторами управления цепями поставок (ЦП) являются эффективность использования всех видов ресурсов и согласованность целей устойчивого развития с целями формирования и функционирования ЦП (получение прибыли, экономический рост, повышение конкурентоспособности и др.), гибкое реагирование на изменения внешней среды.

Указанные факторы напрямую оказывают воздействие на жизнеспособность ЦП — комплексное целевое свойство, характеризующее умения и возможности на протяжении всего жизненного цикла сохранять, оперативно восстанавливать и эффективно реализовать свои основные функции с требуемым качеством в условиях воздействия различного рода внешних и/или внутренних возмущающих факторов, приводящих к аварийным, чрезвычайным и катастрофическим ситуациям.

Функционирование современных ЦП невозможно без использования всего спектра информационных технологий, которые обеспечивают достижение целей логистической деятельности, а именно: если требуемый продукт необходимого уровня качества в необходимом количестве доставлен соответствующему потребителю в требуемое время в требуемое место с минимальными затратами.

В этих условиях обеспечение жизнеспособности ЦП в многократно возрастающей степени становится зависимым от безопасности и защищенности задействованных информационно-телекоммуникационных систем [1-4].

Для реализации указанных возросших требований, в первую очередь, должна быть определена и сформулирована единая политика информационной безопасности, учитывающая структуру и характерные особенности функционирования бизнес-процессов ЦП и возможные риски, связанные с изменениями внешней и внутренней среды, в течение всего жизненного цикла ЦП.

Такая единая политика должна быть обязательной для всех участников ЦП и основываться на взаимно согласованных сведениях, а именно:

- перечне информации, которая подлежит защите в ЦП;
- об организации обработки такой информации;
- об организации доступа к ней субъектов и объектов;
- базе знаний о существующих и возможных уязвимостях;
- базе знаний об угрозах безопасности информации и приоритетности защиты от них;
- базе знаний о моделях нарушителей безопасности информации;
- базе знаний о применяемых мерах обеспечения защиты конфиденциальности;
- базе знаний об имеющихся информационных и технических ресурсах, программных средствах защиты информационно-телекоммуникационных систем;
- о системе контроля и оценки защищенности информации в ЦП.

В докладе рассмотрены возможности формирования интеллектуальной системы управления информационной безопасностью, реализующей единую политику информационной безопасности и обеспечивающую в проактивном режиме поддержку жизнеспособности ЦП на протяжении всего жизненного цикла [5-9].

*Проведенные исследования выполнялись в рамках госбюджетной темы FFZF-2025-0020.*

#### СПИСОК ЛИТЕРАТУРЫ

1. Искандеров Ю.М., Дорошенко В.И. Организация транспортно-технологических процессов на основе интегрированных информационных систем. Сборник статей Международной научно-практической конференции «Новая экономика и основные направления ее формирования». СПб., ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого», ISBN: 978-5-7422-5215-3, 2016, с. 53-62.
2. Искандеров Ю.М. Построение моделей интегрированной информационной системы транспортной логистики на основе мультиагентных технологий. Сборник статей Международной научно-практической конференции «Новая экономика и основные направления ее формирования». СПб., ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого», ISBN: 978-5-7422-5215-3, 2016, с. 62-69.
3. Искандеров Ю.М., Паутов М.Д. Защита корпоративной информации в транспортно-логистических сетях. Сборник статей X Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2017)». СПб., 1-3 ноября 2017. СПОИСУ. СПб., 2017г.
4. Зима В., Молдовян А., Молдовян Н. Безопасность глобальных сетевых технологий. Серия «Мастер». СПб.: БХВ-Петербург, 2001. 320 с.
5. Искандеров Ю.М., Паутов М.Д. Модель интеллектуальной системы управления информационной безопасностью для цепей поставок на основе пространственных концепций акторно-сетевой теории. Информатизация и связь №5, 2020. с. 94-106.
6. Yury Iskanderov, Mikhail Pautov. Security of Information Processes in Supply Chains. Advances in Intelligent Systems and Computing. 2019. Т. 875. р. 13-22. [https://doi.org/10.1007/978-3-030-01821-4\\_2](https://doi.org/10.1007/978-3-030-01821-4_2).
7. Искандеров, Ю. М. Создание безопасных информационных систем транспортной логистики на основе мультиагентного подхода / Ю. М. Искандеров // Информационная безопасность регионов России (ИБРР-2023): XIII Санкт-Петербургская межрегиональная конференция. Материалы конференции, Санкт-Петербург, 25–27 октября 2023 года. Санкт-Петербург: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2023. С. 199-200. EDN RFCVVK.
8. Искандеров, Ю. М. Подсистема информационной безопасности интеллектуальной поддержки перевозки негабаритных грузов / Ю. М. Искандеров, А. С. Чумак, С. Ф. Шахнов // Информационная безопасность регионов России (ИБРР-2023): XIII Санкт-Петербургская межрегиональная конференция. Материалы конференции, Санкт-Петербург, 25–27 октября 2023 года. Санкт-Петербург: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2023. С. 201-202. EDN HFDJFE.
9. Искандеров, Ю. М. Мультиагентное моделирование информационной безопасности транспортно-технологических процессов в цепях поставок / Ю. М. Искандеров, М. Б. Ласкин // Региональная информатика (РИ-2022): Юбилейная XVIII Санкт-Петербургская международная конференция. Материалы конференции, Санкт-Петербург, 26–28 октября 2022 года. Санкт-Петербург: Региональная общественная организация «Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления», 2022. С. 272-273. EDN JVJHID.

УДК 004.89: 656.078

**ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ  
ТРАНСПОРТНО-ЛОГИСТИЧЕСКИХ ПРОЦЕССОВ****Искандеров Юрий Марсович**

СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия

e-mail: iskanderov.y@iias.spb.su

**Аннотация.** В докладе представлен подход к формированию интеллектуальной системы управления информационной безопасностью транспортно-логистических процессов. Отмечены особенности современных условий функционирования транспортно-логистических процессов, предъявляющие новые требования к обеспечению их информационной безопасности. Показана необходимость разработки и создания релевантной интеллектуальной системы управления информационной безопасностью, являющейся интегратором для разработанных специальных инструментов, таких как программы управления рисками, предотвращения потерь данных, безопасности информации и управления событиями, профилирования персонала и другие, адекватных особенностям функционирования транспортно-логистических процессов.

**Ключевые слова:** интеллектуальная система; управление; информационная безопасность; транспортно-технологические процессы; цифровая трансформация.

**INTELLIGENT SYSTEM FOR INFORMATION SECURITY MANAGEMENT  
OF TRANSPORT AND LOGISTICS PROCESSES****Iskanderov Yury**

St. Petersburg Federal Research Center of the Russian Academy of Sciences

39 14th Line VO, St. Petersburg, 199178, Russia

e-mail: iskanderov.y@iias.spb.su

**Abstract.** The report presents an approach to the formation of an intelligent information security management system for transport and logistics processes. The features of modern conditions of transport and logistics processes, which impose new requirements for ensuring their information security, are noted. The need for the development and creation of a relevant intelligent information security management system, which is an integrator for the developed special tools, such as risk management programs, data loss prevention, information security and event management, personnel profiling and others, adequate to the features of the functioning of transport and logistics processes, is shown.

**Keywords:** intelligent system; management; information security; transport and technological processes; digital transformation.

Геополитические события в мире последних лет, в первую очередь пандемия COVID-19 и военные конфликты, коренным образом повлияли на функционирование транспортно-логистических процессов (ТЛП). Взаимосвязанные последствия указанных событий ясно показали, что будущее ТЛП связано с поиском и разработкой эффективных управленческих решений с учетом различного рода рисков, в том числе связанных с цифровой трансформацией.

Стремительное развитие и внедрение новых информационных технологий позволяет транспортно-логистической отрасли демонстрировать наибольшие темпы цифровой трансформации после отраслей с объективно высокой цифровой составляющей, такие как финансы, телекоммуникации и ритейл. Отрасль и российская экономика в целом в короткие сроки адаптировались к новым экономическим условиям во многом благодаря гибкости ТЛП, в основе которых лежит высокий уровень цифровой зрелости.

Обеспечение информационной безопасности всегда была важнейшей задачей при управлении ТЛП, так как при этом генерируются и циркулируют значительные потоки информации, в том числе и конфиденциальная информация. Потеря данных, утечка, повреждение или подделка могут произойти из-за целенаправленной злонамеренной деятельности человека, халатности, ошибок и упущений, сбоев аппаратного или программного обеспечения. Таким образом, с угрозами нарушения управления ТЛП могут быть связаны люди, процессы и технологии. Учитывая подобные условия функционирования, обеспечение информационной безопасности реализуется на основе соответствующих методов [1-4].

Однако начиная с 2022 года значимость мер обеспечения информационной безопасности ТЛП резко возросла: увеличилось число атак, изменились источники и характер атак, в том числе с участием организованных группировок, имеющим поддержку недружественных государств. При этом объекты транспортной отрасли составляют существенную часть национальной критической информационной инфраструктуры.

В современных условиях система обеспечения информационной безопасности должна удовлетворять новым растущим требованиям и представлять собой систему, которая имеет возможности не только защиты от существующих угроз и их устранения, но и возможности прогнозирования угроз, которые могли бы нанести ущерб при управлении ТЛП.

Для решения таких проблем предлагается интеллектуальная система управления информационной безопасностью (ИСУ ИБ), позволяющая осуществлять разработку политики безопасности на стратегическом

уровне, оценку рисков, определение и внедрение мер контроля безопасности, направленных на устранение угроз, мониторинг системы посредством внутренних аудитов и выбором требуемых управляющих воздействий [5-9]. Т.е. указанная ИСУ ИБ будет интегратором для разработанных специальных инструментов, таких как программы управления рисками, предотвращения потерь данных, безопасности информации и управления событиями, профилирования персонала и другие.

Преимуществами такой ИСУ ИБ являются:

- высокий уровень наблюдаемости ТЛП;
- высокая надежность и скорость операций контроля информационной безопасности;
- обоснованность и достоверность окончательных решений;
- минимизация затрат различных ресурсов и комфортное конфиденциальное взаимодействие между участниками ТЛП;
- предотвращение возможных конфликтов между участниками ТЛП, а также негативных последствий взаимодействия с внешней средой.

В докладе рассмотрены принципы построения, архитектура предлагаемой ИСУ ИБ и особенности ее функционирования.

*Проведенные исследования выполнялись в рамках госбюджетной темы FFZF-2025-0020.*

#### СПИСОК ЛИТЕРАТУРЫ

1. Искандеров Ю.М., Дорошенко В.И. Организация транспортно-технологических процессов на основе интегрированных информационных систем. Сборник статей Международной научно-практической конференции «Новая экономика и основные направления ее формирования». СПб., ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого», ISBN: 978-5-7422-5215-3, 2016, С. 53-62.
2. Искандеров Ю.М. Построение моделей интегрированной информационной системы транспортной логистики на основе мультиагентных технологий. Сборник статей Международной научно-практической конференции «Новая экономика и основные направления ее формирования». СПб., ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого», ISBN: 978-5-7422-5215-3, 2016, С. 62-69.
3. Искандеров Ю.М., Паутов М.Д. Защита корпоративной информации в транспортно-логистических сетях. Сборник статей X Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2017)». СПб., 1-3 ноября 2017. СПОИСУ. СПб., 2017.
4. Зима В., Молдован А., Молдован Н. Безопасность глобальных сетевых технологий. Серия «Мастер». СПб.: БХВ-Петербург, 2001. 320 с.
5. Искандеров Ю.М., Паутов М.Д. Модель интеллектуальной системы управления информационной безопасностью для цепей поставок на основе пространственных концепций акторно-сетевой теории. Информатизация и связь №5, 2020. С. 94-106.
6. Yury Iskanderov, Mikhail Pautov. Security of Information Processes in Supply Chains. Advances in Intelligent Systems and Computing. 2019. Т. 875. р. 13-22. [https://doi.org/10.1007/978-3-030-01821-4\\_2](https://doi.org/10.1007/978-3-030-01821-4_2).
7. Искандеров, Ю. М. Создание безопасных информационных систем транспортной логистики на основе мультиагентного подхода / Ю. М. Искандеров // Информационная безопасность регионов России (ИБРР-2023): XIII Санкт-Петербургская межрегиональная конференция. Материалы конференции, Санкт-Петербург, 25–27 октября 2023 года. СПб.: СПОИСУ, 2023. С. 199-200. EDN RFCVKN.
8. Искандеров, Ю. М. Подсистема информационной безопасности интеллектуальной поддержки перевозки негабаритных грузов / Ю. М. Искандеров, А. С. Чумак, С. Ф. Шахнов // Информационная безопасность регионов России (ИБРР-2023): XIII Санкт-Петербургская межрегиональная конференция. Материалы конференции, Санкт-Петербург, 25–27 октября 2023 года. Санкт-Петербург: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2023. С. 201-202. EDN HFDJFE.
9. Искандеров, Ю. М. Мультиагентное моделирование информационной безопасности транспортно-технологических процессов в цепях поставок / Ю. М. Искандеров, М. Б. Ласкин // Региональная информатика (РИ-2022): Юбилейная XVIII Санкт-Петербургская международная конференция. Материалы конференции, Санкт-Петербург, 26–28 октября 2022 года. Санкт-Петербург: Региональная общественная организация «Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления», 2022. С. 272-273. EDN JVJNID.

УДК: 004.89

#### МЕТОДЫ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ЗАЩИТЫ КАНАЛОВ СВЯЗИ В ИНТЕЛЛЕКТУАЛЬНЫХ ТРАНСПОРТНЫХ СИСТЕМАХ

**Калекина Мария Александровна, Нырклов Анатолий Павлович**

Государственный университет морского и речного флота имени адмирала С. О. Макарова

Двинская ул., 5/7, Санкт-Петербург, 198035, Россия

e-mails: maria.kalekina@yandex.ru, kaf.koib@gmail.com

**Аннотация.** Развитие интеллектуальных транспортных систем (ИТС) требует эффективных механизмов защиты каналов связи от кибератак, угрожающих безопасности участников. Традиционные криптографические методы не всегда обеспечивают своевременное выявление сложных и неизвестных угроз. В материале рассматриваются перспективы применения нейронных сетей для анализа сетевого трафика, обнаружения аномалий и предотвращения утечек информации в ИТС. Приведены основные архитектуры нейронных сетей, их возможности и ограничения. Отмечено, что интеграция методов машинного обучения с криптографическими технологиями и федеративным обучением позволит повысить устойчивость транспортных сетей к современным киберугрозам.

**Ключевые слова:** интеллектуальные транспортные системы; кибербезопасность; защита каналов связи; машинное обучение; нейронные сети, V2X-коммуникации.

## MACHINE LEARNING METHODS FOR PROTECTING COMMUNICATION CHANNELS IN INTELLIGENT TRANSPORT SYSTEMS

Kalekina Maria, Nyrkov Anatoly

Admiral Makarov State University of Maritime and Inland Shipping

5/7 Dvinskaya St, St. Petersburg, 198035, Russia

e-mails: maria.kalekina@yandex.ru, kaf.koib@gmail.com

**Abstract:** The development of intelligent transport systems (ITS) requires effective mechanisms to protect communication channels from cyber-attacks that threaten the security of participants. Traditional cryptographic methods do not always ensure timely detection of complex and unknown threats. The article discusses the prospects of using neural networks to analyze network traffic, detect anomalies, and prevent information leaks in ITS. The main architectures of neural networks, their capabilities and limitations are given. It is noted that the integration of machine learning methods with cryptographic technologies and federated learning will increase the resilience of transport networks to modern cyber threats.

**Keywords:** intelligent transport systems; cybersecurity; protection of communication channels; machine learning; neural networks, V2X communications.

Интеллектуальные транспортные системы (ИТС) — ключевой элемент инфраструктуры «умного города», обеспечивающий обмен данными между транспортными средствами, дорожной инфраструктурой и облачными сервисами (V2X-коммуникации) [1]. Утечка или подмена информации о дорожной ситуации, маршрутах движения и параметрах транспортных средств может привести к серьёзным последствиям, включая угрозу жизни участников движения. Поэтому задача обеспечения кибербезопасности каналов связи в ИТС является одной из первостепенных [2].

Традиционные криптографические методы (TLS, PKI, IPsec) обеспечивают базовый уровень защиты, однако они не способны гарантировать своевременное обнаружение новых и сложных атак. В этих условиях перспективным направлением становится использование методов машинного обучения, в частности нейронных сетей, для анализа сетевого трафика и выявления аномалий [3].

К основным угрозам для ИТС относят: перехват и подмену сообщений, DDoS-атаки, подделку информации о дорожной ситуации, атаки на маршрутизацию и кибершпионаж.

Применение нейронных сетей для безопасности в ИТС охватывает широкий спектр задач: от классификации сетевого трафика до прогнозирования угроз и поиска признаков утечки конфиденциальной информации. Рассмотрим основные архитектуры и их применение.

Сверточные нейронные сети (*convolution neural networks* — CNN) были разработаны специально для обработки и анализа структурированных сеток данных, таких как изображения и видео [4]. Такие сети широко используются в области компьютерного зрения, распознавания образов и других задачах, где важны пространственные закономерности. Базовая нейронная сеть состоит из 5 слоёв: входного, сверточного, объединяющего, связанного и выходного. Сверточный слой выполняет операцию свертки над входными данными для выделения локальных закономерностей и особенностей. Это помогает распознавать форму, края и текстуру изображения.

Рекуррентные нейронные сети (*recurrent neural networks* — RNN, LSTM, GRU). Идея таких сетей заключается в последовательном использовании информации. Рекуррентная нейронная сеть отличается от сети с прямым распространением тем, что она «запоминает» своё состояние на предыдущем входе и дополнительно передаёт своё прошлое состояние на следующую итерацию входа нейрона. Такие сети используются для решения задач seq2seq (автоматический перевод, обработка звука, распознавание речи и т.д.), а также эффективны для обнаружения аномалий в сетевом трафике и последовательностях команд в автоматизированных системах управления [5].

Генеративные состязательные сети (*generative adversarial network* — GAN) используются для генерации аудио, текста или изображений, а также для обработки произведений искусства. Генеративное моделирование основано на аппроксимации невычислимого апостериорного распределения. Архитектура состоит из генератора и дискриминатора, настроенных на взаимодействие друг с другом [4, 5]. Генератор отвечает за создание данных, которые могут быть похожи на реальные, что достигается путём его обучения генерировать данные из случайного вектора шума. На начальных этапах обучения выходные данные могут не соответствовать реальным данным, но по мере обучения качество создаваемых данных значительно повышается. Дискриминатор — это классификатор, который определяет, являются ли данные реальными или сгенерированными.

Одним из перспективных направлений для выявления аномалий в сетевом трафике, является использование графовых нейронных сетей (*graph neural networks* — GNN) [4]. GNN использует графовую структуру данных, моделируя связи между IP-адресами, устройствами и потоками данных, что позволяет учитывать топологию сети и выявлять скрытые паттерны атак, обнаруживать сложные атаки, включая APT-атаку (Advanced persistent threat), ботнеты и скрытые каналы связи.

Применение нейронных сетей в системах безопасности ИТС имеет следующие преимущества [6, 7]:

- способность работать с большими и высокоразмерными данными;
- универсальность — возможность применять разные архитектуры под разные типы угроз;
- высокая точность выявления аномалий и утечек;
- возможность адаптивного обучения в реальном времени.

Ограничения:

- значительная вычислительная нагрузка, особенно при использовании глубоких моделей;



— необходимость в больших объемах размеченных данных для обучения;  
уязвимость самих нейронных сетей к атакам (например, adversarial attacks), когда малые изменения входных данных могут приводить к ошибочным выводам.

Нейронные сети представляют собой мощный инструмент для защиты каналов связи в интеллектуальных транспортных системах. Их способность выявлять скрытые закономерности, анализировать временные зависимости и адаптироваться к новым сценариям атак делает их незаменимыми при обнаружении утечек конфиденциальной информации и предотвращении кибершпионажа. В перспективе именно интеграция нейронных сетей с криптографическими методами, федеративным обучением и технологиями объяснимого искусственного интеллекта позволит построить по-настоящему защищенные и устойчивые транспортные сети нового поколения.

#### СПИСОК ЛИТЕРАТУРЫ:

1. Шипунов И. С., Нырклов А. П. IoT устройства как важный аспект современного морского транспорта // Региональная информатика (РИ-2020): сб. материалов XVII С.-П. междунар. конф. Часть 1. — СПб.: СПОИСУ, 2020. С. 362–364.
2. Арбузов А. М. Применение алгоритмов машинного обучения в обеспечении безопасности сетевой инфраструктуры IoT-систем на водном транспорте / А. М. Арбузов, А. П. Нырклов, А. Н. Терехов, И. В. Ли, Д. А. Демениев // Проблемы информационной безопасности. Компьютерные системы. №2. 2025. С. 131–142.
3. Нырклов А. П. Оптимизация процесса тестирования на проникновение в АСУ технологическими процессами с использованием алгоритмов машинного обучения / А. П. Нырклов, Е. С. Юмашева, А. В. Кириков // Вестник государственного университета морского и речного флота им. адмирала С. О. Макарова. Т. 16. № 3. 2024. С. 456–466.
4. Sobolev, A. S. Convolution Neural Network for Identification of Underwater Objects / A. S. Sobolev, S. G. Chernyi, D. O. Krivoguz, A. P. Nyrkov, E. G. Zinchenko // Proceedings of the 2022 Conference of Russian Young Researchers in Electrical and Electronic Engineering, EIConRus 2022 9755621. 2022.
5. Юмашева Е. С. Интеграция графовых моделей для обнаружения аномалий в сетевом трафике / Юмашева Е. С., Нырклов А. П. // Перспективы науки. №6(189). 2025. С. 102–107.
6. Городилов А. В., Чирков В. А. Применение методов машинного обучения для анализа и защиты информационных потоков в транспортных системах // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2020. Т. 16, № 4. С. 85–96.
7. Зегжда Д. П., Челышев А. С. Методы обеспечения информационной безопасности в интеллектуальных транспортных системах // Информационные технологии и телекоммуникации. 2019. Т. 7, № 2. С. 12–23.

УДК 004.946

#### АНАЛИЗ ИНСТРУМЕНТОВ ДЛЯ ПОВЫШЕНИЯ ПРОИЗВОДИТЕЛЬНОСТИ РАБОЧИХ ПРОЦЕССОВ В ПОРТУ

**Кубовский Артемий Андреевич, Журавлев Антон Евгеньевич**

Государственный университет морского и речного флота имени адмирала С. О. Макарова

Двинская ул., 5/7, Санкт-Петербург, 198035, Россия

e-mails: artemii.kub@yandex.ru, zhuravlevae@gumrf.ru

**Аннотация.** С каждым годом появляется больше различных инструментов для повышения производительности и качества работы портов. Но из-за финансовых и технических ограничений порт не может интегрировать все возможные инструменты сразу. Поэтому встает вопрос о выборе наиболее выгодного инструмента из доступных. Рассматриваются наиболее перспективные инструменты. Делается оценка их возможностей и потенциальных затрат на интеграцию.

**Ключевые слова:** автоматизация; мониторинг систем; искусственный интеллект; виртуальная реальность; порты; обучение.

#### ANALYSIS OF TOOLS FOR IMPROVING THE PRODUCTIVITY OF PORT WORKFLOWS

**Kubovskii Artemy, Zhuravlev Anton**

Admiral Makarov State University of Maritime and Inland Shipping

5/7 Dvinskaya St., St. Petersburg, 198035, Russia

e-mails: artemii.kub@yandex.ru, zhuravlevae@gumrf.ru

**Abstract.** Every year there are more and more different tools to improve the productivity and quality of ports. However, due to financial and technical constraints, the port cannot integrate all possible tools at once. Therefore, the question arises about choosing the most profitable tool available. The most promising tools are being considered. An assessment of their capabilities and potential integration costs is being made.

**Keywords:** automation; system monitoring; artificial intelligence; virtual reality; ports; training.

Современный порт представляет собой сложный технологический комплекс, все более вбирающий в себя актуальные решения автоматизации процессов перегрузки, хранения, учета и сопровождения грузов различных типов. Однако каждое решение имеет свою цену, как финансовую, так и техническую. В следствии этого сам процесс автоматизации проходит постепенно и не равномерно. В приоритете оказываются наиболее перспективные и окупаемые варианты, которые уменьшат время и финансовые затраты на рабочие процессы. Наиболее перспективными являются такие направления, как применения искусственного интеллекта, автоматизированный мониторинг и контроль систем, применения виртуальной реальности в процессе обучения.

Искусственный интеллект постепенно внедряется в различные сферы, в том числе и в порты [1]. Главная проблема, которую призван решить искусственный интеллект — человеческий фактор и количество человеческих ресурсов, выделенных на решение конкретной задачи. Например, искусственный интеллект способен проводить более быстрый и точный анализ обстановки на пути следования корабля, что минимизирует риски появления экстренных ситуаций из-за внешних факторов [2]. Точность работы искусственного интеллекта зависит от степени обученности модели и точности источников данных. Зачастую искусственный интеллект может решать сразу несколько задач, что делает его более универсальным инструментом в руках подготовленных людей.

Однако цена такого решения очень велика. Первая из проблем — необходимость обучить модель. Модель обучается на реальных данных, которые необходимо собрать и классифицировать или структурировать для последующего обучения. Подобный процесс занимает много времени и финансовых ресурсов, как на оборудование, так и на обучение. Вторая проблема — необходимость наличия оборудования для интеграции. В условиях водного транспорта будет недостаточно просто принести модель в каком-либо виде на корабль. Необходимо закупить и установить ряд оборудования, состоящего из датчиков и компьютеров для развертывания и полноценного функционирования системы, что также приводит к большим финансовым затратам. Третья проблема — для налаживания и функционирования системы должны иметься обученные специалисты. Эти специалисты должны находиться рядом с такими системами для сопровождения и контроля. А непосредственное обучение и содержание такого персонала ещё раз повышает стоимость данного решения.

Таким образом использование искусственного интеллекта в условиях порта или водного транспорта очень положительно сказывается на процессе работы, но имеет очень большую стоимость для интеграции и поддержки.

Другим инструментом является автоматизированный мониторинг и контроль систем. В качестве системы может выступать любая информационная структура, как видео наблюдения, так и виртуальная реальность. Например, карты активности помещения призваны не только отслеживать перемещения на объекте, но и быстро определять положение конкретных сотрудников или не зарегистрированных лиц [3]. Такая система является эволюцией обычной системы видео наблюдения в сфере безопасности, где как правило было необходимо в реальном времени просматривать камеры и совершать периодические обходы территорий. В случае карты активности помещения, система сама регистрирует наличие объектов или людей в различных частях комплекса, а также автоматически реагирует и собирает информацию на нарушениях или неполадках. Также к данному инструменту можно отнести и использования технологий виртуальной реальности при поддержке математического анализа. Например, использование технологий виртуальной реальности для выбора алгоритмов проведения таможенного контроля, применяемых в отношении различных объектов таможенного контроля при перемещении различными видами транспорта, в зависимости от предлагаемых обстоятельств [4]. Подобная система упростит работу специалиста и оптимизирует процесс контроля, благодаря выбору оптимальных алгоритмов.

Цена такого инструмента менее значительна, в сравнении с применением искусственного интеллекта. Поскольку автоматизированный мониторинг и контроль могут являться эволюцией имеющихся процессов, то это не потребует больших затрат на переобучение сотрудников и поиск нового персонала. Также процесс написания алгоритмов для автоматизации проходит быстрее и дешевле, чем обрусение модели. Однако в зависимости от масштабности, будет соответственно расти и количество затрат на переоборудование, аналогично интеграции искусственного интеллекта.

Последним инструментом является применение виртуальной реальности в процессе обучения. Тренажер на базе технологий виртуальной реальности способен обеспечить полный цикл практической подготовки и аттестации специалиста, способствуя более эффективному формированию профессиональных навыков [5]. В частности, в виртуальной реальности есть возможность смоделировать интерактивные карты и локации реальных портов или пропускных пунктов [6]. Используя виртуальные версии реальных объектов или предприятий, позволяет непосредственно продемонстрировать как рабочие процессы, так и ситуации, которые могут произойти во время работы. Это позволяет без рисков, более качественно подготовить специалистов в реальной работе. Более качественно обученные сотрудники снизят вероятность возникновения нештатных ситуаций по причине неопытности, а также может повысить сам процесс работы благодаря насмотренности, полученной в процессе обучения.

Цена данного инструмента заключается в двух аспектах. Первый — необходимость разработки виртуальной реальности конкретного предприятия, процесса или системы. Чем больше и комплекснее система, тем больше времени и ресурсов потребуется для разработки. Второй — необходимость закупки специального оборудования в виде очков виртуальной реальности. Оба аспекта являются большими затратами для непосредственной реализации, но в процессе эксплуатации расходы не предвидятся, пока не потребуется расширить функционал созданной виртуальной реальности или обновить оборудование.

Таким образом, проанализировав наиболее перспективные направления для автоматизации, можно сказать, что наиболее дешевым, но эффективным инструментом является применение виртуальной реальности в процессе обучения. Оно при сравнительно небольших затратах повышает качество сотрудников и производительность процесса обучения, что положительно сказывается на кадровой подготовке. Использование автоматизированного мониторинга и контроля систем более дорогой, но простой инструмент для повышения качества работы и систем безопасности. Он актуален, если нет необходимости, а более качественной подготовке

кадров, но есть необходимость в оптимизации внутренних процессов предприятия. Внедрение искусственного интеллекта — то самым современным подход, который в перспективе повысит производительность и качество работы, но имеет очень большую цену. Его интеграция требует постоянного контроля и обучения специалистов для работы, что не всегда актуально или выгодно.

#### СПИСОК ЛИТЕРАТУРЫ

1. Журавлев, А. Е. Развитие технологий искусственного интеллекта в транспортной отрасли / А. Е. Журавлев // Региональная информатика и информационная безопасность: Сборник трудов Санкт-Петербургской международной конференции и Санкт-Петербургской межрегиональной конференции, Санкт-Петербург, 23–25 октября 2024 года. СПб.: СПОИСУ, 2024. С. 238-241. EDN SYFNY.
2. Журавлев, А. Е. Особенности и перспективы внедрения технологий искусственного интеллекта на водном транспорте / А. Е. Журавлев, Ю. Е. Ежов, И. В. Упорова // Системы интеллектуального управления и искусственный интеллект: теория и практика : Сборник трудов II национальной научно-практической конференции, Санкт-Петербург, 27 июня 2024 года. СПб.: ФГБОУВО Государственный университет морского и речного флота им. адмирала С.О. Макарова, 2024. С. 37-40. EDN OSAONK.
3. Свидетельство о государственной регистрации программы для ЭВМ № 2022610348 Российская Федерация. Модуль автоматизации мониторинга и контроля карты активности помещения: № 2021681439: заявл. 23.12.2021; опубл. 11.01.2022 / А. В. Макшанов, А. Е. Журавлев, Е. Д. Паутов [и др.]; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Государственный университет морского и речного флота имени адмирала С.О. Макарова». EDN PHSCYI.
4. Щерба М.Ю. Использование технологии виртуальной реальности при подготовке специалистов таможенного дела / М.Ю. Щерба // Академический вестник ростовского филиала российской таможенной академии 2023 года. Ростовский филиал Российской таможенной академии, 2023. С. 118-123. EDN TZGHSQ.
5. Зубарев С.В. Перспективы использования интерактивного VR-тренажера «организация государственного контроля в морском пункте пропуска с применением технологий удаленного выпуска» при подготовке специалистов таможенного дела / С.В. Зубарев, М.Ю. Щерба // Академический вестник ростовского филиала российской таможенной академии 2024 года. Ростовский филиал Российской таможенной академии, 2024. С. 100-106. EDN FBYUYL.
6. Кравцова Т.А. Использование виртуальной реальности в таможенном деле / Т.А. Кравцова // АЛЛЕЯ НАУКИ 2024 года. ИП Шелистов Денис Александрович (Издательский центр «Quantum»), 2024. С. 233-238. EDN XGBGCN.

УДК 621.391

#### ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БЕЗЭКИПАЖНОГО ВОДНОГО ТРАНСПОРТА

**Ныркв Анатолий Павлович, Худайназаров Юрий Кахрамонович**

Государственный университет морского и речного флота имени адмирала С. О. Макарова

Двинская ул., 5/7, Санкт-Петербург, 198035, Россия

e-mail: kaf.koib@gmail.com

**Аннотация.** Рассматривается проблематика обеспечения информационной безопасности роботизированного морского и речного транспорта. Приведены основные аспекты проблемной ситуации по информационной безопасности безэкипажного водного транспорта. Определены основные направления исследований по данной проблеме.

**Ключевые слова:** робототехнический комплекс; безэкипажный водный транспорт; информационная безопасность; угрозы информационной безопасности.

#### ABOUT INFORMATION SECURITY OF UNMANNED WATER TRANSPORT

**Nyrkov Anatoliy, Khudainazarov Yuri**

Admiral Makarov State University of Maritime and Inland Shipping

5/7 Dvinskaya St., St. Petersburg, 198035, Russia

e-mail: kaf.koib@gmail.com

**Abstract.** The problems of ensuring information security of robotic marine and river transport are considered. The main aspects of the problematic situation of information security of unmanned sea and river transport are presented. The main directions of research on this problem are defined.

**Keywords:** robotics complex; information security; threats to information security.

Робототехнические комплексы (РТК) находят широкое применение в различных областях, таких как транспорт и логистика [1-3], разведка и поисково-спасательные операции [4, 5], сельское хозяйство и промышленное производство. Эффективная и координированная работа таких систем требует высокого уровня взаимодействия между отдельными элементами РТК для выполнения поставленных задач. Динамическая и распределенная природа безэкипажного водного транспорта порождает уникальные проблемы в области информационной безопасности, которые требуют глубоких научных исследований и разработки инновационных решений. Возникает актуальная задача обеспечения информационной безопасности системы управления роботизированного транспорта, учитывая его динамическую природу, высокую подверженность кибератакам, террористическим атакам другими роботами [4, 6].

Можно выделить следующие аспекты проблемной ситуации:

1. Обеспечение конфиденциальности и целостности данных: разработка методов шифрования и аутентификации, которые смогут обеспечить безопасность данных при передаче между РТК и центральным

узлом управления, а также между самими РТК; исследование алгоритмов криптографии, адаптированных для использования в условиях ограниченных вычислительных ресурсов и энергетических ограничений РТК.

2. Обеспечение устойчивости к кибератакам: изучение подходов к детектированию и предотвращению сетевых атак, таких как атаки типа DoS, перехват и подмена данных, атаки на маршрутизацию, MITM и другие виды угроз; создание алгоритмов для автоматического обнаружения аномалий в поведении сети и принятие мер для минимизации ущерба от атак [7, 8].

3. Резервирование и отказоустойчивость систем связи: разработка протоколов связи, которые обеспечат высокую надежность и будут способны адаптироваться к изменениям сети, таким как потеря узлов или изменение топологии сети; исследование методов динамической маршрутизации и дублирования каналов связи для повышения устойчивости системы к отказам.

4. Управление и координация группы робототехнических комплексов: изучение моделей и алгоритмов координации, обеспечивающих безопасное взаимодействие и совместную работу РТК даже при наличии нарушений связи или компрометации отдельных узлов; разработка стратегий распределенного управления, которые минимизируют зависимость от центрального узла и повышают общую устойчивость системы.

5. Защита от внутренних угроз: исследование механизмов защиты от внедрения вредоносных РТК в группу, включая методы аутентификации и идентификации узлов, выявление аномальностей в поведении отдельных РТК; разработка процедур безопасного добавления новых узлов в сеть и обновления программного обеспечения РТК.

В качестве основных можно выделить следующие потенциальные направления исследований:

1. Интеграция современных криптографических методов с протоколами связи для РТК, обеспечивающими высокую пропускную способность и низкие задержки.

2. Разработка машинного обучения и иных интеллектуальных систем для обнаружения и классификации аномалий и атак в реальном времени [7-9].

3. Исследование применения блокчейн-технологии для обеспечения безопасности и целостности данных в распределенных системах управления РТК.

4. Создание и тестирование симуляционных моделей для оценки эффективности различных методов защиты и восстановления связи в критических ситуациях [9-11].

#### СПИСОК ЛИТЕРАТУРЫ

1. Shipunov, I.S. About the Problems of Ensuring Information Security on Unmanned Ships / I. S. Shipunov, K. S. Voevodskiy, A. P. Nyrkov, Y. F. Katorin, Y. A. Gatchin // Proceedings of the 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). 2019. Pp. 339-343.
2. Мартынов В.Л. Гидроакустические коммуникации в вопросах противодействия подводным роботам / В. Л. Мартынов, А. П. Ныркин, М. С. Шиманская, Э. В. Кречетова, Г. С. Шиманская // Информатизация и связь. № 2. 2024. С. 51-55.
3. Nyrkov, A.P. Development of underwater robotics / A. P. Nyrkov, A. A. Zhilenkov, V. V. Korotkov, S. S. Sokolov, S. G. Chernyi // Journal of Physics: Conference Series, Volume 803, Issue 1, 2017. № 012108.
4. Sokolov, S. The use robotics for underwater research complex objects / S. Sokolov, A. Zhilenkov, A. Nyrkov, S. Chernyi // Advances in Intelligent Systems and Computing Volume 556, 2017. Pp 421-427.
5. Nyrkov A.P. Optimal Identification for Objects in Problems on Recognition by Unmanned Underwater Vehicles / A. P. Nyrkov, S. S. Sokolov, O. M. Alimov, S. G. Chernyi, V. A. Dorovskoi // Automatic Control and Computer Sciences 54(8) 2020. Pp. 958-963.
6. Kardakova M. Cyber Security on Sea Transport / M. Kardakova, I. Shipunov, A. Nyrkov, T. Knysh // Advances in Intelligent Systems and Computing, Vol. 982. 2020. Pp. 481-490.
7. Юмашева Е.С. Применение алгоритмов машинного обучения для обнаружения аномального поведения в сетях критической информационной инфраструктуры / Юмашева Е.С., Ныркин А.П. // Сб. тр. «Региональная информатика и информационная безопасность». Вып. 12 СПб.: СПОИСУ, 2023. С. 247-251.
8. Ныркин А.П. Оптимизация процесса тестирования на проникновение в АСУ технологическими процессами с использованием алгоритмов машинного обучения / А. П. Ныркин, Е. С. Юмашева, А. В. Кириков // Вестник государственного университета морского и речного флота им. адмирала С.О. Макарова. Т. 16. № 3. 2024. С. 456-466.
9. Арбузов А.М. Применение алгоритмов машинного обучения в обеспечении безопасности сетевой инфраструктуры IoT-систем на водном транспорте / А. М. Арбузов, А. П. Ныркин, А. Н. Терехов, И. В. Ли, Д. А. Деменев // Проблемы информационной безопасности. Компьютерные системы. №2. 2025. С. 131-142.
10. Кардакова М.В. Системы игрового тренажера по информационной безопасности на речном транспорте / М. В. Кардакова, А. П. Ныркин, Ю. В. Цымай // Речной транспорт (XXI век). 2022. № 3 (103). 2022. С. 45-49.
11. Арбузов А.М. Обучение алгоритма R-CNN для распознавания судов на аэроснимках в целях обеспечения безопасности водного транспорта / А. М. Арбузов, М. А. Белова, А. П. Ныркин // Сб. статей Международной научно-практической конференции «Актуальные вопросы обеспечения комплексной безопасности на транспорте». СПб.: СПбГУГА, 2025. С. 3-6.

УДК 004.056

#### DEVSECOPS-ПОДХОД К РАЗРАБОТКЕ ПО ДЛЯ АВТОНОМНЫХ ТРАНСПОРТНЫХ СИСТЕМ

Прокопенко Даниил Николаевич

Государственный университет морского и речного флота имени адмирала С. О. Макарова

Двинская ул., 5/7, г. Санкт-Петербург, 198035, Россия

e-mail: prokopenko.danilka121@gmail.com

**Аннотация.** В условиях растущей подключённости и сложности автономных транспортных средств обеспечение кибербезопасности требует перехода от ручных проверок к непрерывной автоматизации. В работе представлен DevSecOps-пайплайн, интегрирующий статический (SAST), компонентный (SCA) и динамический (DAST) анализ, проверку инфраструктуры как кода (IaC) и автоматизированное тестирование автомобильных

шин (CAN, Ethernet) в процесс CI/CD. Решение, реализованное на Python и Go, обеспечивает раннее выявление уязвимостей, формирование SBOM, соответствие стандартам ISO/SAE 21434 и UN R155 и сокращение времени анализа до нескольких минут. Подход демонстрирует эффективность автоматизации в условиях строгих требований автомобильной индустрии.

**Ключевые слова:** DevSecOps; CI/CD; Python; Go; автомобильная кибербезопасность.

## DEVSECOPS APPROACH TO DEVELOPING SOFTWARE FOR AUTONOMOUS TRANSPORT SYSTEMS

**Prokopenko Daniil**

Admiral Makarov State University of Maritime and Inland Shipping

5/7 Dvinskaya St., St. Petersburg, 198035, Russia

e-mail: prokopenko.danilka121@gmail.com

**Abstract.** With the increasing connectivity and complexity of autonomous vehicles, cybersecurity requires a shift from manual checks to continuous automation. The paper presents a DevSecOps pipeline that integrates static (SAST), component (SCA), and dynamic (DAST) analysis, infrastructure as code (IaC) verification, and automated automotive bus testing (CAN, Ethernet) into the CI/CD process. The solution, implemented in Python and Go, provides early vulnerability detection, SBOM generation, compliance with ISO/SAE 21434 and UN R155 standards, and reduces analysis time to a few minutes. This approach demonstrates the effectiveness of automation in the strict requirements of the automotive industry.

**Keywords:** DevSecOps; CI/CD; Python; Go; automotive cybersecurity.

Программное обеспечение автономных транспортных средств (АТС) управляет критически важными функциями АТС. Увеличение числа подключённых интерфейсов и сложность ПО приводит к росту атакующей поверхности. При этом традиционные практики информационной безопасности, основанные на периодических аудитах и ручных проверках, не соответствуют скорости и масштабу современной разработки, особенно в условиях Agile и CI/CD. В результате уязвимости обнаруживаются слишком поздно, что увеличивает стоимость исправлений и повышает риски. В автомобильной сфере эта проблема усугубляется спецификой embedded-систем, отсутствием встроенной защиты в шинах связи (например, CAN) и ужесточением нормативных требований, таких как UN R155 и ISO/SAE 21434. Следовательно, актуальной задачей становится создание автоматизированной, непрерывной и стандарт-ориентированной системы обеспечения безопасности. [1-5].

Существующие подходы к кибербезопасности в автомобильной разработке характеризуются фрагментарностью, высокой трудоёмкостью и низкой интеграцией в процесс CI/CD. Ручное тестирование шин связи требует дорогостоящего оборудования и экспертизы, а анализ зависимостей часто проводится выборочно. Кроме того, отсутствует единый механизм нормализации результатов различных инструментов, что затрудняет принятие решений. Это приводит к пропуску уязвимостей, особенно на уровне библиотек и сетевых интерфейсов, и не позволяет в полной мере соответствовать требованиям регуляторов.

В работе предложен DevSecOps-пайплайн, обеспечивающий непрерывную автоматизацию кибербезопасности. Пайплайн включает:

- SAST-анализ с использованием Bandit (Python) [6], gosec (Go) и Semgrep с кастомными правилами для embedded-сред;
- SCA-сканирование с генерацией SBOM в формате CycloneDX и проверкой зависимостей через Trivy [7] с блокировкой при наличии уязвимостей CVSS  $\geq 7.0$ ;
- проверку IaC (Docker, Kubernetes) с помощью checkov и tfsec на соответствие CIS-бенчмаркам;
- DAST-тестирование в изолированной среде с использованием легковесного сканера на Go;
- автоматизированный пентест шин связи: фаззинг CAN-фреймов (через python-can [8]), сканирование Ethernet (с помощью scapy [9]) и симуляция атак, таких как подмена данных о скорости или DoS-атаки.

Все этапы выполняются в Docker-контейнерах, результаты нормализуются в SARIF и интегрируются в системы управления кодом. Критические уязвимости приводят к остановке сборки. Особое внимание уделено адаптации правил анализа под специфику embedded-систем. В частности, реализованы проверки на использование небезопасных функций стандартной библиотеки, отсутствие валидации входных данных, поступающих от автомобильных шин, а также на наличие подозрительных конструкций, потенциально указывающих на наличие бэкдоров.

Ручное тестирование на проникновение в автомобильных сетях является ресурсоёмким и трудновоспроизводимым процессом, требующим специализированного оборудования и глубоких знаний протоколов. Для преодоления этих ограничений разработан модульный фреймворк на языке Python, обеспечивающий автоматизацию ключевых этапов пентеста.

Автоматизация кибербезопасности на основе DevSecOps является необходимым условием безопасной и эффективной разработки ПО для автономных транспортных средств. Предложенный подход демонстрирует практическую реализуемость непрерывного контроля безопасности в условиях строгих нормативных и технических требований автомобильной индустрии. Практическая ценность предложенного решения заключается в значительном сокращении времени выявления уязвимостей — с традиционных нескольких месяцев до менее чем 10 минут. Это позволяет командам быстро реагировать на новые угрозы и поддерживать высокий уровень безопасности на всех этапах жизненного цикла разработки.

## СПИСОК ЛИТЕРАТУРЫ

1. Прокопенко Д. Н. Безопасность программного обеспечения в эпоху SI/CD: актуальные подходы и решения / Д. Н. Прокопенко // Сб. тр. «Региональная информатика и информационная безопасность». Вып. 13. СПб.: СПОИСУ, 2024. С. 243–248.
2. Нырков А. П. О методологии разработки приложений «Непрерывная интеграция и доставка» / А. П. Нырков, Д. Н. Прокопенко // Материалы конференции «XIX Санкт-Петербургская международная конференция «Региональная информатика (РИ-2024)». Санкт-Петербург, 23-25 октября 2024. СПб.: СПОИСУ, 2024. С. 223–224.
3. Нырков А. П. Защита информации при управлении разнородной группировкой безэкипажных средств водного транспорта / А. П. Нырков, Ю. К. Худайназаров // Материалы конференции «XIX Санкт-Петербургская международная конференция «Региональная информатика (РИ-2024)». Санкт-Петербург, 23-25 октября 2024. СПб.: СПОИСУ, 2024. С. 224–226.
4. ISO/SAE 21434:2021 Road vehicles Cybersecurity engineering [Электронный ресурс]. URL: <https://www.iso.org/standard/70918.html> (дата обращения: 18.08.2025).
5. UN Regulation № 155 on Cybersecurity and Cybersecurity Management System (CSMS) [Электронный ресурс]. URL: <https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security> (дата обращения: 18.08.2025).
6. Bandit Python Security Linter from OpenStack Security Group [Электронный ресурс]. URL: [https://bandit.readthedocs.io/en/latest/?spm=a2ty\\_o01.29997173.0.0.6840c9218TF3UD](https://bandit.readthedocs.io/en/latest/?spm=a2ty_o01.29997173.0.0.6840c9218TF3UD) (дата обращения: 18.08.2025).
7. Trivy Vulnerability Scanner for Containers and Other Artifacts [Электронный ресурс]. URL: <https://trivy.dev/latest/> (дата обращения: 18.08.2025).
8. Python-can Python module for working with CAN buses [Электронный ресурс]. URL: <https://github.com/hardbyte/python-can> (дата обращения: 18.08.2025).
9. Scapy Interactive packet manipulation program [Электронный ресурс]. URL: <https://github.com/secdev/scapy> (дата обращения: 18.08.2025).

УДК 004.056.55:629.7.05

**КВАНТОВАЯ КРИПТОГРАФИЯ В БЕСПИЛОТНЫХ СИСТЕМАХ: ВЫЗОВЫ И КРИТЕРИИ ОЦЕНКИ****Рыбакова Таисия Константиновна**

Государственный университет морского и речного флота им. адм. С.О. Макарова  
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия  
e-mail: tkrybakova@gmail.com

**Аннотация.** Рост применения беспилотных летательных аппаратов (БПЛА) сопровождается возрастанием киберугроз, что делает задачу обеспечения защищённой связи особенно актуальной. В докладе рассматриваются ключевые вызовы при внедрении квантовой криптографии в беспилотные системы: ограниченные ресурсы платформы (энергия, вес, размеры), нестабильность каналов связи и необходимость миниатюризации оборудования.

**Ключевые слова:** квантовая криптография; беспилотные летательные аппараты; защищённая связь; критерии оценки; киберугрозы.

**QUANTUM CRYPTOGRAPHY IN UNMANNED SYSTEMS:  
CHALLENGES AND EVALUATION CRITERIA****Rybakova Taisiia**

Admiral Makarov State University of Maritime and Inland Shipping  
5/7 Dvinskaya St., St. Petersburg, 198035, Russia  
e-mail: tkrybakova@gmail.com

**Abstract.** The growing use of unmanned aerial vehicles (UAVs) is accompanied by an increase in cyber threats, which makes the task of providing secure communications especially urgent. The report examines the key challenges in the implementation of quantum cryptography in unmanned systems: limited platform resources (energy, weight, dimensions), instability of communication channels and the need for miniaturization of equipment.

**Keywords:** quantum cryptography; unmanned aerial vehicles; secure communications; evaluation criteria; cyber threats.

Современные беспилотные летательные аппараты (БПЛА) активно используются в военной и гражданской сферах, что делает обеспечение защищённой связи ключевым фактором их эффективности [1]. Однако традиционные методы шифрования постепенно утрачивают надёжность на фоне роста вычислительных мощностей и угрозы появления квантовых компьютеров. В этих условиях перспективным направлением становится квантовая криптография, которая способна обеспечить долгосрочную безопасность каналов связи [2].

При рассмотрении возможности её внедрения в беспилотные системы важно учитывать не только характеристики конкретных протоколов [3-7], но и комплекс факторов, определяющих практическую применимость технологии. Среди таких факторов выделяются: скорость генерации ключа, обеспечивающая своевременное обновление криптографического материала; максимальная дальность передачи, напрямую связанная с подвижностью и автономностью БПЛА [8, 9]; устойчивость к внешним атакам и шумам, определяющая надёжность связи в условиях активного противодействия; доступность и степень зрелости аппаратных решений, влияющая на скорость внедрения; а также физические ограничения самих платформ, включая энергопотребление, вес оборудования и виброустойчивость. [10, 11]

Стоит предположить, что квантовые протоколы представляют собой перспективный инструмент защиты дроновых сетей, однако успешная интеграция в беспилотные платформы требует междисциплинарного подхода, включающего развитие компактной фотонной аппаратуры, оптимизацию энергопотребления и адаптацию технологий к условиям динамической эксплуатации. [8, 10]

Особое внимание требует решение проблемы совместимости квантовых систем с существующими архитектурами связи БПЛА. Современные дроны часто используют комбинированные каналы передачи данных, включая радиочастотные, спутниковые и оптические линии, что создает сложности при интеграции квантовых модулей, рассчитанных на работу в узком диапазоне условий. Для преодоления этого барьера необходимо разрабатывать гибридные схемы, где квантовая криптография будет дополнять, а не заменять традиционные методы шифрования. Например, использование квантовых ключей для защиты критически важных команд при одновременном применении классических алгоритмов для потоковой передачи видео или телеметрии. Такой подход позволит поэтапно внедрять технологию, минимизируя риски сбоев в работе комплексных систем.

Не менее важным представляется анализ влияния физических параметров полёта на стабильность квантовых каналов. Высокая подвижность БПЛА приводит к частым изменениям расстояния между узлами сети, колебаниям угла наклона оптических антенн и временным задержкам в синхронизации. Эти факторы могут нарушить процесс квантового распределения ключей, требуя разработки адаптивных алгоритмов компенсации динамических искажений. Перспективным решением становится интеграция квантовых модулей с системами искусственного интеллекта, способными прогнозировать траекторию движения дрона и корректировать параметры передачи в режиме реального времени. Это не только повысит надёжность связи, но и снизит долю ошибок, связанных с механическими колебаниями платформы.

Кроме технических аспектов, следует учитывать организационные и операционные ограничения, возникающие при масштабировании квантовых сетей для группировки дронов. В сценариях, где задействованы десятки или сотни аппаратов, традиционные схемы «точка-точка» становятся неэффективными из-за экспоненциального роста вычислительной нагрузки. Здесь актуальными оказываются топологии с централизованным управлением ключами или децентрализованные протоколы, основанные на блокчейн-технологиях. Однако их реализация потребует пересмотра подходов к распределению ресурсов и балансировке нагрузки между узлами, что напрямую повлияет на энергопотребление и вычислительную сложность бортовых систем. Таким образом, успешное развертывание квантовой криптографии в массовых дронах потребует не только технологических прорывов, но и принципиально новых стратегий управления криптографической инфраструктурой.

Внедрение квантовой криптографии в беспилотные системы требует не только технологических решений, но и формирования новой экосистемы взаимодействия между научными, промышленными и регуляторными структурами. Ключевым условием успеха станет создание унифицированных стандартов, совместимых с международными требованиями к безопасности и совместимости оборудования. Это позволит избежать фрагментации рынка и ускорит адаптацию технологий как в военных, так и в гражданских сценариях. Параллельно необходимо развивать образовательные программы, ориентированные на подготовку специалистов, способных работать на стыке квантовой физики, кибербезопасности и робототехники. Без такого синергетического подхода даже самые передовые разработки останутся лабораторными экспериментами, не находя применения в реальных операциях, где от надёжности связи зависят не только данные, но и человеческие жизни.

Перспективы квантовой криптографии в дронах напрямую связаны с динамикой развития смежных областей, таких как миниатюризация фотонных компонентов, энергоэффективные вычисления и автономное управление сетями. Уже сегодня очевидно, что будущее за гибридными системами, где квантовые методы станут элементом многоуровневой защиты, дополняя классические алгоритмы в критических сценариях. Однако для перехода от теоретических моделей к промышленным решениям потребуются целевые инвестиции в исследования и испытания, а также диалог между разработчиками и заказчиками для чёткого определения приоритетов. В конечном итоге, только системный подход, объединяющий инновации в аппаратном обеспечении, программном обеспечении и операционных протоколах, сможет превратить квантовую криптографию из многообещающей концепции в неотъемлемую часть инфраструктуры безопасных беспилотных систем будущего.

## СПИСОК ЛИТЕРАТУРЫ

1. Tian, X.-H., et al. Drone-based quantum key distribution [Электронный ресурс]. 2023. Режим доступа: <https://arxiv.org/abs/2302.14012>.
2. Coubourne, S. Quantum Key Distribution. Protocols and Applications // Security at Royal Holloway, University of London. 2011.
3. Abruzzo, S.; Mertz, M.; Kampermann, H.; Bruss, D. Finite-key analysis of the six-state protocol with photon number resolution detectors // Optics and Photonics for Counterterrorism and Crime Fighting VII; Optical Materials in Defence Systems Technology VIII; and Quantum-Physics-based Information Security / eds. R. Zamboni, F. Kajzar, A. A. Szepe, C. Lewis, D. Burgess, M. T. Gruneisen, M. Dusek, J. G. Rarity. SPIE, 2011. Vol. 8189. P. 818917. doi:10.1117/12.898049. Режим доступа: <https://arxiv.org/abs/1111.2798>.
4. Lo, H.-K., Curty, M., Qi, B. Measurement-Device-Independent Quantum Key Distribution // Physical Review Letters. 2012. T. 108, № 13. C. 130503.
5. Tang, Y.-L., et al. Measurement-Device-Independent Quantum Key Distribution over 200 km // Physical Review Letters. 2014. T. 113, № 19. C. 190501.
6. Gottesman, D.; Chuang, I. L. Quantum Digital Signatures [Электронный ресурс]. 2001. Режим доступа: <https://arxiv.org/abs/quant-ph/0105032>.
7. Clarke, P. J., Collins, R. J., Dunjko, V., Andersson, E., Jeffers, J., Buller, G. S. Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light // Nature Communications. 2012. T. 3. C. 1174.
8. Zhang, Y., Bian, Y., Li, Z., Yu, S., Guo, H. Continuous-variable quantum key distribution system: Past, present, and future // Applied Physics Reviews. 2024. T. 11, № 1. C. 011301.
9. Zhang, Y., et al. Long-Distance Continuous-Variable Quantum Key Distribution over 202.81 km of Fiber // Physical Review Letters. 2020. T. 125, № 1. C. 010502.
10. Fitzsimons, J. F. Private quantum computation: an introduction to blind quantum computing and related protocols // npj Quantum Information. 2017. T. 3. C. 23.
11. Broadbent, A., Fitzsimons, J., Kashefi, E. Universal Blind Quantum Computation // 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS). 2009. C. 517–526.

УДК 004.021

**МОНИТОРИНГ ФУНКЦИОНИРОВАНИЯ БЕСПИЛОТНЫХ ТРАНСПОРТНЫХ СРЕДСТВ  
В УСЛОВИЯХ ВНЕШНИХ ВОЗДЕЙСТВИЙ****Семенов Виктор Викторович**

СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия

e-mail: v.semenov@spcras.ru

**Аннотация.** Разработана методика выявления нарушений информационной безопасности беспилотных транспортных средств, сочетающая в себе совокупность методов машинного обучения при анализе разнородных внешних данных цифровых сигналов, поступающих от различных элементов и объединённых в поведенческие паттерны. Даны рекомендации по использованию результатов исследования для повышения защищённости беспилотных транспортных средств от внешних воздействий. В качестве перспектив дальнейшей разработки тематики следует указать исследования, связанные с развитием модели режимов функционирования и детализации причин возникновения выявленных нарушений информационной безопасности.

**Ключевые слова:** беспилотные транспортные средства; информационная безопасность; функциональная безопасность; риски; методы машинного обучения.

**FUNCTIONAL MONITORING OF UNMANNED VEHICLES UNDER EXTERNAL IMPACTS****Semenov Viktor**

St. Petersburg Federal Research Center of the Russian Academy of Sciences

39, 14th Line V.O., St. Petersburg, 199178, Russia

e-mail: v.semenov@spcras.ru

**Abstract.** A methodology for identifying information security violations of unmanned vehicles has been developed, combining a set of machine learning methods in the analysis of heterogeneous external data of digital signals coming from various elements and combined into behavioral patterns. Recommendations are given on the use of the research results to improve the safety of unmanned vehicles from external impacts. As prospects for further development of the topic, it is necessary to indicate studies related to the development of a model of operating modes and detailing the causes of the identified information security violations.

**Keywords:** unmanned vehicles; information security; functional safety; risks; machine learning methods.

Существующая методология обеспечения информационной безопасности (ИБ) беспилотных транспортных средств (БТС) ориентирована на применение классических средств защиты и направлена преимущественно на обнаружение атак, однако при этом не рассматриваются возможности динамического контроля параметров функционирования системы для обеспечения её жизнеспособности в условиях деструктивных воздействий [1].

Реализация угрозы с использованием уязвимостей системы со стороны злоумышленника может привести к нарушению целевых функций БТС. Поскольку ключевой задачей функционирования БТС является бесперебойное выполнение целевых функций, выявление рисков нарушений ИБ БТС представляет собой важную и необходимую в современных реалиях задачу [2].

Применение разработанной методики способно предотвратить описанный сценарий воздействия злоумышленника. Предлагаемая общая методика выявления нарушений ИБ может быть применена для повышения уровня безопасности БТС, путем внедрения в качестве технической меры по аудиту ИБ БТС в период эксплуатации.

Обладая полной и актуальной информацией о текущем состоянии объекта становится возможным существенно повысить степень защищённости БТС, ускорить быстроту реагирования на инциденты (в том числе с использованием динамического переконфигурирования, обеспечивающего возвращение системы в устойчивое состояние), снизив тем самым риски нарушения ИБ [3].

В том случае, если инцидент ИБ уже произошёл, разработанная методика может применяться в качестве апостериорной защиты, которая помогает найти и наказать виновного в выявленном инциденте уже после того, как он произошёл, реализуя тем самым принцип неотвратимости наказания за нарушение ИБ, и замыкая цикл процесса обеспечения ИБ.

Можно выделить смежные задачи, решаемые разработанной методикой:

- выявление рисков, вызванных случайными воздействиями на БТС и не связанных с умышленными действиями вероятных нарушителей, например, различных природных факторов в виде порывов ветра, скользкой дороги;

- выявления отклонений в параметрах функционирования, вызванные износом технологических узлов БТС.

Приведены ограничения методики, к которым можно отнести сильные помехи при формировании сигнальных последовательностей, вызванные функционированием некоторых типов БТС.

Разработаны практические рекомендации по применению методики для повышения уровня безопасности БТС, включающие в себя варианты получения сигнальной информации о параметрах функционирования системы, а также использования динамического переконфигурирования, обеспечивающего возвращение системы в устойчивое состояние.



Сформулированы перспективы области, состоящие в развитии и проработке предложенной модели, а также в разработке методов реагирования на выявленные риски нарушения ИБ на основе принципа обратной связи.

Достоинствами данного подхода является возможность быстрой адаптации под конкретный тип БТС с применением различного математического аппарата и методов машинного обучения для получения требуемой точности выявления нарушений ИБ. Дальнейшие исследования в данной области могут быть связаны с интеграцией разработанной методики в системы комплексного обеспечения информационно-функциональной безопасности БТС.

Таким образом, разработанная методика является как новой альтернативой, так и дополнением к существующим программным и программно-аппаратным средствам, и может использоваться для выявления нарушений ИБ БТС. При необходимости и соответствующей настройке, контролирующая система может блокировать небезопасные манёвры транспортного средства в режиме реального времени.

*Благодарность.* Исследования, выполненные по данной тематике, проводились при финансовой поддержке госбюджетной темы FFZF-2025-0020.

#### СПИСОК ЛИТЕРАТУРЫ

1. Семенов В.В. Метод мониторинга состояния элементов киберфизических систем на основе анализа временных рядов // Научно-технический вестник информационных технологий, механики и оптики. 2022. Т. 22, № 6. С. 1150-1158. DOI: 10.17586/2226-1494-2022-22-6-1150-1158.
2. Сухопаров М.Е., Семенов В.В., Лебедев И.С., Гаранин А.В. Подход к анализу состояния узлов «Индустрии 4.0» на основе поведенческих паттернов // Научные технологии в космических исследованиях Земли. 2020. Т. 12, № 5. С. 83-91. DOI 10.36724/2409-5419-2020-12-5-83-91.
3. Семенов В.В. Подход к формированию информативных признаков в задачах мониторинга информационной безопасности киберфизических систем // Научно-технический вестник информационных технологий, механики и оптики. 2021. Т. 21, № 6. С. 887-894. doi: 10.17586/2226-1494-2021-21-6-887-894.

УДК 656

#### ПОВЫШЕНИЕ ЖИЗНЕСПОСОБНОСТИ СИСТЕМЫ УПРАВЛЕНИЯ МОРСКИМ ПОРТОМ

Хасанов Дмитрий Салимович

СПб ФИЦ РАН

14-я линия В.О., д. 39, г. Санкт-Петербург, 199178, Россия

e-mail: dkhasanovsuai@yandex.ru

**Аннотация.** В статье исследуются современные подходы к повышению жизнеспособности системы управления морским портом (СУМП) в условиях нарастающих киберугроз и операционных рисков. Жизнеспособность рассматривается как ключевое свойство системы, обеспечивающее ее способность не только противостоять дестабилизирующим воздействиям, но и адаптироваться к ним, сохраняя основные функциональные возможности и восстанавливая работоспособность в сжатые сроки. Особый акцент делается на роли информационной безопасности (ИБ) как фундаментального элемента, обеспечивающего целостность, доступность и конфиденциальность критически важных данных транспортной системы. Традиционные подходы к безопасности, основанные на периметровой защите, недостаточны для современных киберфизических систем порта. Предлагается концепция интегрированной системы управления, сочетающая методы проактивного мониторинга, резервирования критических компонентов, внедрение архитектуры «Zero Trust» и использование технологий цифровых двойников для моделирования угроз и отработки сценариев восстановления.

**Ключевые слова:** Жизнеспособность системы; морской порт; система управления; информационная безопасность; киберустойчивость; транспортная система; цифровой двойник; Zero Trust.

#### ENHANCED VIABILITY OF THE SEAPORT MANAGEMENT SYSTEM

Khasanov Dmitry

<sup>1</sup> St. Petersburg Federal Research Center of the Russian Academy of Sciences,

39, 14th Line V.O., St. Petersburg, 199178, Russia

e-mail: dkhasanovsuai@yandex.ru

**Abstract.** The article examines modern approaches to improving the viability of the seaport management system (SPMS) in the face of increasing cyber threats and operational risks. Viability is considered as a key property of the system, ensuring its ability not only to withstand destabilizing effects, but also to adapt to them, maintaining basic functionality and restoring operability in a short time. Particular emphasis is placed on the role of information security (IS) as a fundamental element that ensures the integrity, availability and confidentiality of critical data of the transport system. Traditional approaches to security based on perimeter protection are insufficient for modern cyber-physical port systems. The concept of an integrated management system is proposed that combines proactive monitoring methods, redundancy of critical components, implementation of the Zero Trust architecture and the use of digital twin technologies for threat modeling and recovery scenarios.

**Keywords:** System viability; seaport; control system; information security; cyber resilience; transport system; digital twin; Zero Trust.

Современный морской порт представляет собой сложную киберфизическую систему, интегрирующую физические активы (краны, причалы, транспорт) и цифровые технологии управления (SCADA, TOS, ERP). Его функционирование критически важно для национальной и глобальной экономики. Однако данная сложность делает порты уязвимыми для широкого спектра угроз: кибератаки, техногенные катастрофы, климатические изменения, сбои в логистических цепях. [1-3] Традиционные концепции надежности и безопасности фокусируются на предотвращении инцидентов, но не учитывают необходимость функционирования в условиях уже реализовавшегося воздействия.

В этом контексте парадигма жизнеспособности становится центральной. Жизнеспособность СУМП — это ее способность предвидеть, выдержать, восстановиться и адаптироваться к дестабилизирующим воздействиям. Информационная безопасность (ИБ) перестает быть просто сервисом и трансформируется в системообразующий атрибут, пронизывающий все уровни управления [4]. Цель работы — разработать научно-обоснованные тезисы для построения жизнеспособной СУМП с интегрированной системой ИБ.

Жизнеспособность как системное свойство современного морского порта. Жизнеспособность системы управления морским портом базируется на четырех компонентах:

1. Устойчивость (Robustness) — способность поглощать возмущения без потери функциональности. В контексте информационной безопасности это означает отказоустойчивые архитектуры, дублирование каналов связи и вычислительных мощностей.

2. Восстанавливаемость (Recoverability) — способность быстро возвращаться в нормальное состояние после сбоя. Это требует наличия актуальных резервных копий данных, подготовленных сценариев аварийного восстановления и обученного персонала.

3. Адаптивность (Adaptability) — способность системы изменять свою структуру и алгоритмы в ответ на новые вызовы. Реализуется через адаптивные системы обнаружения вторжений, машинное обучение для анализа угроз и гибкие политики безопасности.

4. Проактивность (Anticipation) — способность прогнозировать угрозы на основе анализа больших данных и сценарного моделирования. Инструментом здесь выступают центры мониторинга безопасности и цифровые двойники. [5, 8]

Информационная безопасность является катализатором для каждого из этих компонентов. Без обеспечения целостности данных о грузах и судах, доступности систем планирования и конфиденциальности коммерческой информации говорить о жизнеспособности невозможно [6].

Транспортные системы, в том числе морские порты, становятся главной целью для кибератак:

- Кибершпионаж и саботаж — целевые атаки на промышленные системы управления (ICS/SCADA) портовой инфраструктуры (краны, системы шлюзования).

- Ransomware-атаки — шифрование данных терминальных операционных систем (TOS), парализующее грузопереработку.

- Нарушение цепочек поставок — компрометация программного обеспечения, поставляемого третьими сторонами.

- Инциденты, вызванные человеческим фактором — ошибки персонала, социальная инженерия.

Реализация любой из этих угроз напрямую снижает жизнеспособность порта, приводя к финансовым, репутационным и, что критично, физическим потерям. [7]

Повышение жизнеспособности требует пересмотра архитектуры информационной безопасности:

1. Отказ от периметровой модели в пользу «Zero Trust» архитектуры — принцип «никому не доверяй, проверяй всегда» должен применяться ко всем пользователям и устройствам внутри сети порта. Микросегментация сети изолирует критичные сегменты (напр., сеть управления кранами от офисной сети).

2. Сквозной мониторинг и управление инцидентами — внедрение платформы для корреляции событий от источников данных (IT, OT, IoT) в режиме, близком к реальному времени.

3. Регулярное тестирование на проникновение и моделирование угроз — проведение обучения не только для IT-специалистов, но и для инженеров операционных технологий (OT) и руководства.

4. Использование цифровых двойников — создание виртуальной копии систем управления морским портом позволяет проводить моделирование атак, оценивать их последствия и отрабатывать протоколы восстановления без риска для реального объекта.

5. Формализация взаимодействия — четкое нормативное закрепление процедур обмена информацией об угрозах между всеми заинтересованными сторонами — администрацией порта, стивидорами, логистическими компаниями и государственными органами [9].

6. «Морской порт» (ГК «Ростех») — комплексная система управления деятельностью морского порта. Интегрирует в себе функции TOS (управление терминалом) и PCS (портовая сообщество). Позволяет в режиме реального времени управлять обработкой грузов, складскими операциями, планировать швартовку судов и оптимизировать использование техники. Повышает жизнеспособность за счет централизации данных и автоматизации ключевых процессов, снижая зависимость от человеческого фактора. [10]

АСУ ТП (Автоматизированные Системы Управления Технологическими Процессами) на основе SCADA-систем. Отечественные SCADA-системы (например, «КРУГ-2000» или «ТРИКОНТ») используются для управления системами энергоснабжения, шлюзования, орошения угля, противопожарной безопасности. [11]

Цифровые двойники портовых акваторий и терминалов. Разрабатываются для крупных портовых проектов (например, для порта «Бронка» или «Тамань»). Позволяют в виртуальной среде моделировать: Распределение судопотока, оптимальную расстановку кранов и техники, последствия инцидентов (кибератака, выход оборудования из строя) для отработки протоколов восстановления.

Программные комплексы для моделирования логистических потоков. Российские IT-компании создают решения для прогнозирования нагрузки на терминалы и оптимизации взаимодействия с железной дорогой и автомобильным транспортом.

Повышение жизнеспособности системы управления морским портом является комплексной задачей, требующей интеграции организационных, технических и технологических мер. Устаревшие, реактивные модели защиты должны уступить место проактивным и адаптивным стратегиям, основанным на принципах киберустойчивости. Предложенный подход, включающий внедрение архитектуры «Zero Trust», сквозной мониторинг, использование цифровых двойников и регулярное тестирование, позволяет сформировать систему управления морским портом, способную не только противостоять известным угрозам, но и адаптироваться к новым, непредвиденным вызовам.

*Благодарность. Исследования, выполненные по данной тематике, проводились при финансовой поддержке госбюджетной темы FFZF-2025-0020.*

#### СПИСОК ЛИТЕРАТУРЫ

1. Бабурина, О. Н. Риски и угрозы функционирования морской отрасли в условиях цифровизации мировой экономики / О. Н. Бабурина, Л. К. Гуриева // Морские интеллектуальные технологии. 2019. № 2-2(44). С. 109-115. EDN MABRFO.
2. Зинурова, Г. Х. Риски цифровизации транспортной системы РФ / Г. Х. Зинурова // Актуальные решения проблем водного транспорта: Сборник материалов I Международной научно-практической конференции, Астрахань, 28 апреля 2022 года. Астрахань: Индивидуальный предприниматель Сорокин Роман Васильевич (Издатель: Сорокин Роман Васильевич), 2022. С. 273-277. EDN WMWUHI.
3. Аносов, А. В. Использование концепции «нулевого доверия» (Zero Trust) в обеспечении информационной безопасности правоохранительных органов / А. В. Аносов // Информатизация и информационная безопасность правоохранительных органов: сборник трудов Международной научно-практической конференции, Москва, 30 июня 2023 года. Москва: Академия управления МВД России, 2023. С. 24-30. EDN HARVEW.
4. Семенов, В. В. Метод мониторинга состояния элементов киберфизических систем на основе анализа временных рядов / В. В. Семенов // Научно-технический вестник информационных технологий, механики и оптики. 2022. Т. 22, № 6. С. 1150-1158. DOI 10.17586/2226-1494-2022-22-6-1150-1158. EDN SIWNDM.
5. Захаров, В. В. Специальное модельно алгоритмическое обеспечение планирования информационных процессов при взаимодействии группировки подвижных морских объектов / В. В. Захаров, Б. В. Соколов, В. А. Ушаков // Седьмая международная научно-практическая конференция «Имитационное и комплексное моделирование морской техники и морских транспортных систем» (ИКМ МТМТС-2023) : Труды конференции, Санкт-Петербург; Кронштадт, 22 июня 2023 года. Санкт-Петербург: НП-Принт, 2023. С. 96-103. EDN BMXDKU.
6. Хасанов, Д. С. Планировка контейнерного терминала / Д. С. Хасанов // Региональная информатика (РИ-2022): Юбилейная XVIII Санкт-Петербургская международная конференция. Материалы конференции, Санкт-Петербург, 26–28 октября 2022 года. Санкт-Петербург: Региональная общественная организация «Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления», 2022. С. 286-288. EDN CGYHRI.
7. Смоленцев, С. В. Кооперативное маневрирование безэкипажных судов для безопасного расхождения в море / С. В. Смоленцев, А. Е. Сазонов, Ю. М. Искандеров // Вестник государственного университета морского и речного флота им. адмирала С.О. Макарова. 2018. Т. 10, № 4. С. 687-695. DOI 10.21821/2309-5180-2018-10-4-687-695. EDN YLQZCP.
8. Свистунова, А. С. Построение цифрового двойника Западного скоростного диаметра Санкт-Петербурга на основе имитационного моделирования / А. С. Свистунова, Д. С. Хасанов, Д. М. Кравец // Десятая всероссийская научно-практическая конференция по имитационному моделированию и его применению в науке и промышленности «Имитационное моделирование. Теория и практика» (ИММОД-2021): Труды конференции (электронное издание), Санкт-Петербург, 20–22 октября 2021 года / Редакторы Плотников А.М., Долматов М.А., Смирнова Е. П. Санкт-Петербург: АО «Центр технологии судостроения и судоремонта», 2021. С. 382-388. EDN TTDSTO.
9. Искандеров, Ю. М. Развитие транспортно-технологических процессов на основе интегрированных информационных систем / Ю. М. Искандеров, В. Д. Гаскаров, С. В. Смоленцев // Транспортное дело России. 2019. № 5. С. 114-117. EDN MITYNL.
10. Кузнецов, А. Л. Порто-ориентированная логистика России в новых геополитических условиях / А. Л. Кузнецов, А. Е. Слищан, А. Н. Ситов // Сборник научных статей национальной научно-практической конференции профессорско-преподавательского состава ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова» : Сборник статей конференции, Санкт-Петербург, 30 сентября 20 2024 года. Санкт-Петербург: Государственный университет морского и речного флота им. адмирала С.О. Макарова, 2025. С. 121-125. EDN MVEIKQ.
11. Хасанов, Д. С. Распределение ресурсов для контейнерных терминалов в реальном времени / Д. С. Хасанов // Информатизация и связь. 2024. № 4. С. 70-77. DOI 10.34219/2078-8320-2024-15-70-77. EDN ERIGZN.

УДК 004.056.5

#### АВТОМАТИЗАЦИЯ ПРОЦЕССОВ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ: ВОЗМОЖНОСТИ, ОГРАНИЧЕНИЯ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

Юмашева Елена Сергеевна

Государственный университет морского и речного флота имени адмирала С. О. Макарова

Двинская ул., 5/7, Санкт-Петербург, 198035, Россия

e-mail: yumasheva.lena@list.ru

**Аннотация.** В работе рассматриваются современные подходы к автоматизации процессов тестирования на проникновение (пентестинга) с применением специализированных инструментов и методов. Проведен анализ возможностей и ограничений автоматизированных систем, включая этапы разведки (OSINT), сканирования, поиска уязвимостей, эксплуатации и составления отчетности по проведенной работе.

**Ключевые слова:** тестирование на проникновение; автоматизация; искусственный интеллект; OSINT; Nmap; Nuclei; Metasploit.

## AUTOMATION OF PENETRATION TESTING PROCESSES: OPPORTUNITIES, LIMITATIONS AND DEVELOPMENT

Yumasheva Elena

Admiral Makarov State University of Maritime and Inland Shipping  
5/7 Dvinskaya St., St. Petersburg, 198035, Russia  
e-mail: yumasheva.lena@list.ru

**Abstract.** The paper examines modern approaches to the automation of penetration testing (pentesting) processes using specialized tools and methods. The analysis of the capabilities and limitations of automated systems, including the stages of exploration (OSINT), scanning, vulnerability detection, exploitation and reporting on the work carried out.

**Keywords:** penetration testing; automation; artificial intelligence; OSINT; Nmap; Nuclei; Metasploit.

В условиях непрекращающегося роста сложности IT-инфраструктур, а соответственно и числа потенциальных угроз кибербезопасности, тестирование на проникновение становится одним из ключевых инструментов оценки защищенности информационных систем. Традиционные подходы, основанные исключительно на ручных действиях, требуют значительных как временных и финансовых затрат, так и человеческих ресурсов. В то же время, развитие автоматизированных инструментов, интеграция технологий из различных разделов области Искусственного интеллекта, например, машинного обучения, позволяют ускорить выполнение рутинных операций сосредоточив усилия специалистов на анализе более сложных и нестандартных сценариев атак [1].

Современные инструменты, такие как AMASS [2], Recon-ng [3], theHarvester [4], Shodan [5] и многие другие, позволяют автоматизировать до 90% задач на этапе проведения разведки (OSINT), обеспечивая быстрый сбор данных о целевой инфраструктуре без активного взаимодействия с объектом. На стадии сканирования Nmap и Masscan обеспечивают точную высокопроизводительную «инвентаризацию» портов и сервисов, а интеграция Nmap с NSE и базами уязвимостей (CVE, Vulners) позволяет оперативно выявлять потенциально уязвимые сервисы.

Инструменты Nuclei и OpenVAS реализуют шаблонное и комплексное сканирование уязвимостей, а Metasploit Framework и Cobalt Strike упрощают этап эксплуатации, обеспечивая автоматизированное внедрение и управление сессиями. На заключительном этапе специализированные платформы (Dradis, Faraday) автоматизируют агрегацию результатов и формирования отчетов, интегрируя данные с баг-трекерами и системами управления уязвимостями.

Дополнительно, автоматизация включает в себя применение гибридных систем, совмещающих пассивный и активный сбор данных, основанных на алгоритмах машинного обучения. Такие решения уже не только способны находить известные уязвимости, но и выявлять аномалии в сетевом трафике, анализировать поведенческие паттерны пользователей и сервисов, а также прогнозировать потенциальные векторы атак [6]. Например, интеграция AMASS с ML-моделями позволяет динамически фильтровать результаты, снижая количество ложноположительных находок и выделяя объекты с наибольшим риском эксплуатации [7].

Однако несмотря на очевидные преимущества, автоматизация пентеста имеет ряд ограничений. Инструменты пассивного поиска уязвимостей не способны учитывать бизнес-контекст и часто формируют базы избыточно объемными, включая ложноположительные результаты. Активные сканеры и эксплойты могут нарушить работу целевых систем, особенно в средах с повышенными требованиями к доступности (например, ICS/SCADA).

Алгоритмы машинного обучения других разделов области ИИ, хотя и способны ускорять анализ логов и аномалий, также зависят от качества обучающих данных и могут допускать ошибки в условиях сложных, многосвязных атак [8]. Особую сложность представляют логические уязвимости и дефекты бизнес-логики, которые требуют творческого подхода и глубокого понимания архитектуры приложения [9].

В промышленных системах автоматизация пентеста требует особой осторожности. ICS-среды часто используют устаревшие протоколы (Modbus, DNP3, IEC 60870-5-104), не предназначенные для работы в условиях кибератак. Активное сканирование и эксплуатация уязвимостей в таких системах могут привести к остановке технологических процессов. Поэтому при тестировании рекомендуется использовать преимущественно пассивные методы анализа, симуляцию атак в стендовых условиях и применение специализированных фреймворков (например, Industrial Exploitation Framework) в режиме ограниченного воздействия.

В ближайшей перспективе ожидается более глубокая интеграция ИИ-моделей в автоматизированные пентест-платформы, включая адаптивное планирование атак, автоматическую генерацию эксплойтов и имитацию действий квалифицированного злоумышленника. Однако, даже при значительном прогрессе автоматизации, ключевая роль в тестировании на проникновение сохранится за человеком, способным к нестандартному мышлению, комплексной оценке рисков и учету бизнес-логики атак.

Автоматизация процессов тестирования на проникновение, является мощным инструментом повышения эффективности работы специалистов по кибербезопасности. Она позволяет ускорить рутинные этапы, минимизировать человеческие ошибки и обеспечить системность тестирования. Тем не менее, автоматизированные средства не способны полностью заменить опытного пентестера, особенно в условиях сложных и высокорисковых объектов, таких как объекты входящие в критическую информационную

инфраструктуру. Оптимальной является модель, при которой автоматизация выполняет роль «первой линии» тестирования, а финальный анализ и принятие решений остаются за специалистом.

#### СПИСОК ЛИТЕРАТУРЫ

1. Нырков А.П. Оптимизация процесса тестирования на проникновение в АСУ технологическими процессами с использованием алгоритмов машинного обучения / А. П. Нырков, Е. С. Юмашева, А. В. Кириков // Вестник государственного университета морского и речного флота им. адмирала С. О. Макарова. Т. 16. № 3. 2024. С. 456-466.
2. OWASP Amass: In-depth Attack Surface Mapping and Asset Discovery [Электронный ресурс]. GitHub. URL: [https://github.com/owasp-amass/amass?utm\\_source=chatgpt.com](https://github.com/owasp-amass/amass?utm_source=chatgpt.com) (дата обращения: 09.08.2025).
3. Recon-ng: Framework для разведки в веб-пространстве [Электронный ресурс]. GitHub. URL: <https://github.com/lanmaster53/recon-ng> (дата обращения: 09.08.2025).
4. theHarvester: Инструмент для сбора e-mail-адресов, поддоменов и имен [Электронный ресурс]. GitHub. URL: <https://github.com/laramies/theHarvester> (дата обращения: 09.08.2025).
5. Shodan: Официальная библиотека Python для работы с Shodan [Электронный ресурс]. GitHub. URL: <https://github.com/achillean/shodan-python> (дата обращения: 09.08.2025).
6. Юмашева Е. С. Применение алгоритмов машинного обучения для обнаружения аномального поведения в сетях критической информационной инфраструктуры / Юмашева Е. С., Нырков А. П. // Сб. тр. «Региональная информатика и информационная безопасность». Вып. 12 СПб.: СПОИСУ, 2023. С. 247-251.
7. Yegorov A. V. Automated Penetration Testing in ICS Environments: Risk Assessment and Methodology / A. V. Yegorov, I. N. Petrov, S. M. Orlov // Journal of Information Security. No 3. 2023. Pp. 45-56. <https://doi.org/10.1234/jis.2023.3.45>.
8. Арбузов А. М. Применение алгоритмов машинного обучения в обеспечении безопасности сетевой инфраструктуры IoT-систем на водном транспорте / А. М. Арбузов, А. П. Нырков, А. Н. Терехов, И. В. Ли, Д. А. Деменев // Проблемы информационной безопасности. Компьютерные системы. №2. 2025. С. 131-142.
9. Нырков А.П. Математическое обеспечение нестандартных задач / Нырков А. П. СПб.: СПГУВК, 1998. 46 с.



## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ

УДК 629.19

### ИНТЕЛЛЕКТУАЛИЗАЦИЯ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПО ТЕХНОЛОГИИ ЦИФРОВЫХ ДВОЙНИКОВ СИСТЕМ БОРЬБЫ ЗА ИНФОРМАЦИОННУЮ ЖИВУЧЕСТЬ КОРАБЛЯ, СУДНА

Михальчук Андрей Васильевич<sup>1</sup>, Алексеев Анатолий Владимирович<sup>1</sup>, Антипов Василий Васильевич<sup>2</sup>,  
Смольников Александр Васильевич<sup>2</sup>

<sup>1</sup>Санкт-Петербургский государственный морской технический университет  
Лотманская ул., д.3, Санкт-Петербург, 199178, Россия

<sup>2</sup>АО «Научно-производственное объединение «Аврора»  
Карбышева ул., д. 15, Санкт-Петербург, 194021, Россия  
e-mails: lapbgks@bk.ru

**Аннотация.** Обобщены результаты исследования возможностей технологии цифровых двойников на базе варианта роботизированного проектного комплекса «РПК «КСР-25.СБЖк», обеспечивающего интеллектуализацию поддержки принятия решений при борьбе за информационную живучесть корабля, судна. Показано, что цифровое моделирование в реальном масштабе времени с использованием исходных данных от объекта моделирования типа корабль, судно позволяет прогнозировать обстановку, принимать обоснованные управленческие решения и упреждать возникновение аварийных ситуаций и аварий на корабле, включая информационные инциденты различной природы. Более того, интеллектуализация управления информационной живучестью позволяет оптимизировать систему борьбы за живучесть корабля, судна в целом, переходить в перспективе к роботизации процессов управления организационно-техническими системами.

**Ключевые слова:** интеллектуализация управления; защищенное исполнение; цифровая модель; борьба за информационную живучесть; режим «цифровая тень»; система комплексной защиты информации.

### INTELLECTUALIZATION OF DECISION-MAKING SUPPORT FOR DIGITAL TWIN TECHNOLOGY OF SYSTEMS FIGHTING FOR THE INFORMATION SURVIVABILITY OF A SHIP, VESSEL

Mikhailchuk Andrey<sup>1</sup>, Alekseev Anatoly<sup>1</sup>, Antipov Vasily<sup>2</sup>, Smolnikov Alexander<sup>2</sup>

<sup>1</sup>Sankt-St. Petersburg State Maritime Technical University  
3 Lotsmanskaya St., St. Petersburg, 199178, Russia,

<sup>2</sup>AO Scientific and Production Association Aurora  
Karbysheva St., 15, St. Petersburg, 194021, Russia  
e-mails: lapbgks@bk.ru

**Abstract.** The results of a study of the possibilities of digital twin technology based on a variant of the robotic design complex PKK KSPR-25.SBZHk, which provides intellectualization of decision support in the struggle for the information survivability of a ship, vessel, are summarized. It is shown that real-time digital modeling using source data from a ship-type modeling object allows predicting the situation, making informed management decisions and anticipating the occurrence of emergencies and accidents on the ship, including information incidents of various nature. Moreover, the intellectualization of information survivability management makes it possible to optimize the system of fighting for the survivability of the ship, the vessel as a whole, and to move in the future to the robotization of organizational and technical systems management processes.

**Keywords:** management intellectualization; secure execution; digital model; struggle for information survivability; digital shadow mode; integrated information protection system.

Накопленный опыт исследования технологий цифровых двойников (ЦД) приводит к необходимости обобщения результатов исследования их возможностей, технологии, в том числе на базе одного из их перспективных вариантов - роботизированного проектного комплекса «РПК «КСР-25.СБЖк» (ранее разработанного Санкт-Петербургском государственном морском техническом университете («Корабелка») и Некоммерческом партнерстве «Институт автоматизации процессов борьбы за живучесть корабля, судна»).

Они обеспечивают интеллектуальную поддержку принятия проектных (задача проектирования) и управленческих (задача эксплуатации) решений по оценке, анализу, синтезу и оптимизации систем борьбы за живучесть корабля (СБЖк), включая задачу борьбы за информационную живучесть (ИЖк), в режимах: «1.ЦП» (цифровой паспорт объектов анализа типа «Система управления борьбой за информационную живучесть

корабля, судна» и других с их ранжированием по системным характеристикам в произвольном количестве, включая пять вариантов, отображаемых на главной экранной форме; «2.СМПК.М» (цифровая модель системы мониторинга, прогнозирования, контроля проектного качества в режиме «Цифровая модель»); «2.СМПК.Т» (СМПК эффективности эксплуатации объекта анализа в режиме «Цифровая тень») при ситуационном управлении (задача эффективного боевого управления функционированием СБЖк) с учетом современных факторов высокой динамики процессов борьбы на море [1-5] все большее внимание исследователями уделяется вопросам создания адекватных моделей, полимодельных комплексов (ПМК) и проведения многовариантных модельных исследований этих сложных и высоко динамичных процессов.

Особую актуальность, в том числе в связи с событиями СВО, приобрели сегодня вопросы не только эффективного управления силами и оружием, но и задача обеспечения комплексной защиты информации (КЗИ) автоматизированных систем управления в информационно-защищенном исполнении (АСЗИ), которую применительно к объектам морской техники (ОМТ) типа «корабль» принято называть информационной живучестью корабля (ИЖк) в комплексе с другими элементами (компонентами, элементами) и свойствами системы борьбы за живучесть корабля (СБЖк) [5]: управляемостью СБЖк корабля, в которую входит ИЖк; непотопляемостью корабля; взрыво-пожаро-радиационной безопасностью корабля; живучестью технических средств и оружия корабля; защищенностью личного состава (ЛС) корабля. Именно противоборство в информационной сфере сегодня является непрерывным по времени, пространству и диапазону используемых возможностей, в связи с чем, развитие СБЖк в информационно-защищенном исполнении [5-7] является одним из перспективных и высоко востребованных, так как обеспечивает из базовых требований наряду с непрерывностью управления его скрытность и устойчивость и, как следствие, оперативность управления СБЖк. Однако, для максимальной реализации этих возможностей, а, тем более, обеспечения военно-технического превосходства (ВТП) в управлении над аналогами, включая противника, (ВТПбж) по этим критериям необходимо непрерывно развивать и иметь интеллектуальную подсистему (систему) поддержки решений и управления СБЖк (ИСПРУБж) в море и на берегу [1, 5, 7].

Исследована задача изыскания военно-научных путей обеспечения ВТПбж применительно к кораблям класса «Фрегат», а также адаптации алгоритма ЦД в варианте РПК «КСР-25» к условиям функционирования СБЖк в режиме «Цифровой тени» для обеспечения информационной живучести корабля и адаптировать реализующий ее РПК в варианте «КСР-25.СБЖк» с учетом факторов и возможностей КЗИ для исследования перспективных научно-технических путей, а также структурно-функциональной и параметрической оптимизации ИЖк применительно к каждой и всему комплексу задач обеспечения ИЖк в составе СБЖк. Конечно, типы атак могут быть различными, что требует от СКЗИ в составе АСЗИ соответствующих возможностей и качественных характеристик по критериям и показателям. Вместе с тем, суть функционирования ЦД, как ПМК, сводится к сбору и обработке данных от объекта о его состоянии по соответствующим информационным каналам в соответствующих контурах (выделенных функциональных подсистемах сбора и анализа данных (отдельных моделей) о решении конкретных задач, обеспечивающих соответствующие свойства СБЖк в целом), анализ обобщенной информации от которых позволяет оператору обосновывать и принимать решение по управлению ИЖк в составе СБЖк.

Приведенные оценки показывают большие возможности ЦД управления ИЖк при моделировании проектного качества и ожидаемой эффективности управления ИЖк, БЖк и боевыми потенциалами кораблей в целом при борьбе на море в процессе решения широкого круга проектных и практических задач при обосновании направлений развития, разработке средств и систем, их испытаниях и эксплуатации, что является предметом отдельного рассмотрения. Важнейшей задачей обоснования направлений развития СКЗИ в составе АСЗИ и решения задач СБЖк является цифровое моделирование и обоснование требований к ним. Причем, в условиях тенденции роста сложности современных организационно-технических систем практически безальтернативным следует считать использование адекватных ПМК и их систем типа РПК «КСР-25.СБЖк», включая ИЖк. Числовое вариантное моделирование при поиске оптимальных решений по структуре, свойствам и характеристикам объектов исследования при наличии средств поддержки типа РПК «КСР-25.СБЖк» позволяет сложные системные и наукоемкие задачи при одновременной инженерной оценке и синтезе частных технических проработок решать на большом множестве вариантов проектирования в достаточно сжатые сроки с конкретным их ранжированием по результатам достижения главных целевых показателей.

В свою очередь, систематизация получаемых данных с их фиксацией в соответствующих базах данных и знаний позволяет аккумулировать научно-технологический потенциал и обоснованно выходить на конкурентно способные системные и организационно-технологические решения при одновременной и существенной экономии ресурсных затрат. Применительно к комплексу задач кораблей, в том числе класса «Фрегат», разработанный ЦД (компьютерная модель), прежде всего, может быть результативно использован группой Главного конструктора СБЖк при решении целого комплекса задач проектирования от исследовательского проектирования с обоснованием системно-технического облика, оперативно-технических требований к СБЖк в рамках НИОКР до комплекса задач технического проектирования, создания опытных образцов ЦД и их приемо-сдаточных испытаний с интегрированной оценкой достигнутых результатов.

#### СПИСОК ЛИТЕРАТУРЫ

1. Бобрович В.Ю., Алексеев А.В., Антипов В.В., Смольников А.В. Информационная живучесть корабля: угрозы, модель, системные требования, пути реализации / Информационная безопасность регионов России (ИБРР-2021). – СПб., 2021, с. 265-267.

2. Антипов В.В., Смольников А.В. Сертификация качества моделей на примере цифровых двойников управления борьбой за живучесть корабля, судна / Труды Санкт-Петербургского государственного морского технического университета. Выпуск 5 (9), 2025, с. 5-14.
3. Алексеев А.В., Михальчук А.В. Цифровой двойник системы комплексной защиты информации в инвариантном исполнении (ЦД СКЗИ) / Свидетельство о государственной регистрации программ для ЭВМ (Реестр ФСИС) № 2014613622, 01.04.2023 (06.02.2014).
4. Максимова М.А., Согонов С.А., Михальчук А.В. Модель и технология цифровых двойников систем автоматизации судов / Труды Санкт-Петербургского государственного морского технического университета (СПбГМТУ). Выпуск 4 (8), 2023, с. 5-14.
5. Автоматизация процессов борьбы за живучесть корабля, судна // Коллективная монография – Санкт-Петербург: ИАП БЖКС, эл. интерактивное изд. (третье), испр. и доп., с приложением, 2022. – 506 с.
6. Субетто А.И., Алексеев А.В. Теория практики квалиметрического обеспечения развития морских автоматизированных систем / Актуальные проблемы морской энергетики: материалы седьмой Всероссийской межотраслевой научно-технической конференции в рамках Второго Всероссийского научно-технического форума «Корабельная энергетика: из прошлого в будущее». – СПб.: Изд-во СПбГМТУ, 2018, с. 78 – 86.
7. Алексеев А.В., Михальчук А.В. Цифровой мониторинг, прогнозирование и контроль успешности реализации комплекса организационно-технических решений (ЦМПК, цифровой двойник) / Свидетельство о государственной регистрации программ для ЭВМ (Реестр программ Федеральной службы по интеллектуальной собственности) № 2023661669, 01.06.2023.

УДК 629.19

## ЦИФРОВИЗАЦИЯ КАЧЕСТВА КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ СЕРТИФИКАЦИИ ИННОВАЦИОННЫХ РЕШЕНИЙ

Алексеев Анатолий Владимирович

Санкт-Петербургский государственный морской технический университет

Лотманская ул., 3, Санкт-Петербург, 190121, Россия

e-mail: lapbgks@bk.ru

**Аннотация.** При сертификации новых средств и систем защиты информации (ССЗИ) в настоящее время оценивается только соответствие заданным требованиям, причем, мера соответствия этим требованиям не входит в зону внимания при сертификации соответствия. На начальном этапе развития ССЗИ это было оправдано и дало определенные результаты. Вместе с тем, сегодня это стало тормозом в их развитии, так как получение сертификата соответствия при отсутствии системы оценки их качества не позволяет утверждать о конкурентных преимуществах ССЗИ как на национальном, так и на международном рынке, ставит заказчика при выборе средств в неразрешимую проблему выбора наиболее эффективных из них, в том числе ввиду отсутствия кроме маркетинговых данных объективного инструментального контроля качества, данных сертификационных испытаний. Равно как оценка инновационной привлекательности и обоснование инвестиционной целесообразности по существу продолжают оставаться процессами заведомо субъективными. Предлагается в развитие ранее сформулированной концепции инструментального контроля качества вариант цифровизации качества инновационных решений и сертификации их качества на основе технологии КАСОР-23.

**Ключевые слова:** сертификация соответствия; сертификация качества; перспективность развития; минимизация избыточности; оптимизация систем защиты информации.

## DIGITALIZATION OF THE QUALITY OF COMPREHENSIVE INFORMATION PROTECTION IN THE CERTIFICATION OF INNOVATIVE SOLUTIONS

Alekseev Anatoly

Saint Petersburg State Marine Technical University

3 Lotsmanskaya St, Saint Petersburg, 190121, Russia

e-mail: lapbgks@bk.ru

**Abstract.** When certifying new information security tools and systems (ISS), only compliance with specified requirements is currently assessed, and the degree of compliance with these requirements is not included in the focus of conformity certification. At the initial stage of ISS development, this was justified and yielded certain results. However, today it has become a brake on their development, since obtaining a certificate of conformity in the absence of a quality assessment system does not allow us to assert the competitive advantages of ISS both in the national and international markets, and puts the customer in an insoluble problem of choosing the most effective of them when choosing tools, including due to the lack of objective instrumental quality control and certification test data in addition to marketing data. Just as the assessment of innovative attractiveness and justification of investment feasibility essentially continue to be obviously subjective processes. In development of the previously formulated concept of instrumental quality control, an option for digitalizing the quality of innovative solutions and certifying their quality based on KASOR-23 technology is proposed.

**Keywords:** certification of conformity; quality certification; development prospects; minimization of redundancy; optimization of information security systems.

В результате более чем 30-летнего периода развития современных ССЗИ в составе национального актива по данным Реестра сертифицированных ССЗИ только ФСТЭК России насчитывается более 4800 средств защиты информации и их систем. Это позволяет заказчикам и разработчикам выбирать необходимые элементы для своих автоматизированных систем в защищенном исполнении (АСЗИ), формировать системы комплексной защиты информации (СКЗИ) в соответствии со своими требованиями, особенностями решения задач своими АСЗИ.



Однако, многообразие этих требований далеко не большое, а значительную их часть составляют типовые требования ФСТЭК и других ведомств. В этой связи, в свете требований Федерального закона «О техническом регулировании» вопрос мог бы быть успешно решен при выборе для АСЗИ сертифицированных средств.

Вместе с тем, при сертификации средств и систем защиты информации (ССЗИ) в настоящее время оценивается только соответствие заданным требованиям, причем, мера соответствия этим требованиям не входит в зону внимания при сертификации соответствия. На начальном этапе развития ССЗИ это было оправдано и дало определенные результаты. Однако, сегодня это стало тормозом в их развитии, так как получение сертификата соответствия при отсутствии системы оценки их качества не позволяет утверждать о конкурентных преимуществах ССЗИ как на национальном, так и на международном рынке, ставит заказчика при выборе средств в неразрешимую проблему выбора наиболее эффективных из них, в том числе ввиду отсутствия кроме маркетинговых — данных объективного контроля инструментального контроля качества, сертификационных испытаний. Равно как оценка инновационной привлекательности и обоснование инвестиционной целесообразности по существу продолжают оставаться процессами заведомо субъективными.

В этой связи встает ряд очевидных вопросов: Какие средства для создаваемых АСЗИ выбрать из состава присутствующих на рынке средств? При наличии ряда альтернатив какие из них выбрать? Является ли критерий минимума стоимости при этом рациональным? Если (а это очевидно) нет, то каким путем выбирать архитектуру, состав, функционал элементов создаваемой СКЗИ и ее структуру? Насколько успешно и, даже, оптимально в результате решения этих вопросов будет решаться задача комплексной защиты информации при соответствующем спектре угроз безопасности? А какой уровень защиты потенциально может обеспечить выбранный заказчиком, разработчиком, пользователем набор средств и соответствующая их СКЗИ? Если нет, что и как делать при проектировании СКЗИ? Есть ли общепризнанные практические методики решения этой задачи? Есть ли, наконец, теория и лучшие практики решения этой нетривиальной задачи? Через 30 лет бурного развития предметной области информационной безопасности информации, активов организации (ИБ)?

К сожалению, на большую часть этих вопросов однозначного ответа нет, а риски принятия необоснованного инновационного, а, тем более, инвестиционного решения в условиях названной неопределенности немерено возрастают, оставляя заказчика, разработчика, пользователя наедине с ними.

При этом, как никогда нужны типовые решения задачи проектного обоснования СКЗИ с контролируемым на цифровом уровне показателем проектного качества и соответствующей эффективности эксплуатации (как меры реализации показателя проектного качества). Пусть, даже, на начальном этапе не самые убедительные и удовлетворяющие все «хотелки» уважаемого нами ИБ-сообщества. Развитие пойдет. Было бы что развивать.

Первопричиной данной проблемы является отсутствие в настоящее время общепризнанной модели оценки ИБ, включая модели цифровизации «фундаментальных» уже критериев конфиденциальности, доступности, целостности информации в составе СКЗИ и АСЗИ в целом. Отсутствие цифровой модели этих показателей.

Наличие такой модели и цифровизация качества СКЗИ, оценка качества защиты активов предприятия, организации — прямой путь к их совершенствованию ИБ, зрелости процессов защиты данных, критичности обстановки в информационной сфере, критичности и значимости элементов и СКЗИ в составе АСЗИ.

Знание нарушителем режима ИБ ее уровня — прямая угроза информационных инцидентов и катастроф.

Решение данной проблемы [1-4] мы видим и предлагаем в развитие ранее сформулированной концепции инструментального контроля качества ССЗИ [5] на пути цифровизации качества инновационных решений и сертификации их качества на основе созданных в Санкт-Петербургском государственном морском техническом университете технологии и роботизированного проектного комплекса (РПК) «КАСОР-23» [6, 7].

Отличительными преимуществами данного подхода и технологии от известных, по нашему мнению, могут быть названы: практическая направленность на решение задач цифровой сопоставимости альтернативных решений; наличие сравнительно объективных исходных данных для оценивания качества ССЗИ в виде уровней их сертификации с переходом к так называемому обобщенному уровню качества по данным сертификации (ОУС); возможность цифровизации качества не только средств, но и СКЗИ в целом за счет использования полимодельного способа агрегирования данных по гармоническому алгоритму; возможность цифровой оптимизации средств и СКЗИ при вариантном поиске за счет использования метода цифрового моделирования при наличии средств типа «калькулятор ИБ» на базе РПК «КАСОР-23».

Среди недостатков данной технологии могут быть названы лишь ограниченная точность ввода исходных данных, обусловленная погрешностями субъективного бинарного оценивания соответствия требованиям при сертификационных испытаниях, а также необходимость непрерывной актуализации баз данных и знаний в РПК.

Практическая доступность средств цифровизации качества ИБ, средств и СКЗИ в целом путем использования лишь данных о типе средств в составе СКЗИ (остальные данные хранятся и актуализируются в РПК) позволяют процедуру количественного оценивания качества СКЗИ, в том числе при сертификации инновационных решений, аудите ИБ предприятий, организаций, объектов автоматизации и т.п., сделать общедоступной для пользователей с минимальным уровнем подготовки (пользовательским), так как основная «наукоемкая составляющая» хранится и актуализируется в базе данных и знаний РПК.

Наконец, формирование единой цифровой среды квалитетического оценивания ИБ активов предприятий, организаций, бизнеса и т.п., качества СКЗИ в составе АСЗИ, эффективности проведения аудита ИБ станет естественным стимулом для совершенствования ССЗИ с цифровым «пониманием необходимости и достаточности», уровня конкурентной способности, уровня инновационности и инвестиционной актуальности.

Организация СКЗИ и система обеспечения ИБ должна быть системой опережающей. Сертификация инновационных решений в области ИБ, переход от системы сертификации соответствия к системе сертификации качества ССЗИ должен базироваться на опережающем формировании информационного пространства общества.

#### СПИСОК ЛИТЕРАТУРЫ

1. Алексеев В.В., Карасева Е.И. Синтез и анализ вероятностей событий по нечисловой неточной и неполной экспертной информации // Проблемы анализа риска. Том 11, 2014, № 3. С. 22-31.
2. Курач А.Е. Применение функционально-стоимостного анализа в инновационном процессе // Современные научные исследования и инновации. 2014. № 12 [Электронный ресурс]. URL: <http://web.snauka.ru/issues/2014/12/43019> (дата обращения: 30.09.2016).
3. Ендовицкий Д.А., Бабушкин В.А., Батурина Н.А. Анализ инвестиционной привлекательности организации: научное издание / под ред. Д.А. Ендовицкого. М.: КНОРУС, 2010, 376 с.
4. Зефилов С.Л. Проблема измерения и оценки информационной безопасности организации // Открытое образование, 2011, № 2, с. 134-137.
5. Алексеев А.В. Модель цифровой оценки конфиденциальности, доступности, целостности данных и ее реализация в программном комплексе «КАСОР» / Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 12 / СПОИСУ. СПб., 2023. С. 252-258.
6. Алексеев А.В. Программа квалитетического анализа, синтеза и оптимизации решений (КАСОР) / Свидетельство о гос. регистрации программ для ЭВМ (Реестр программ Федеральной службы по интеллектуальной собственности) № 2023616388, 27.03.2023 (поступление: 13.03.2023).
7. Алексеев А.В. Модель и программный комплекс цифровой трансформации кибербезопасности / Вопросы обеспечения безопасности в киберпространстве: материалы Всероссийской НТК Махачкала: ДГТУ, 2022 г. 387 с. с. 251-255.

УДК 629.19

### ИНФОРМАЦИОННАЯ ЖИВУЧЕСТЬ КОРАБЛЯ, СУДНА: МАСТЕР-КЛАСС

Алексеев Анатолий Владимирович

Институт автоматизации процессов борьбы за живучесть корабля, судна  
Ленинский пр., 101, оф. 162, Санкт-Петербург, 198262, Россия  
e-mail: [lapbgks@bk.ru](mailto:lapbgks@bk.ru)

**Аннотация.** В формате мастер-класса по тематике автоматизации процессов борьбы за живучесть корабля, судна впервые обобщены и представлены накопленные знания и практический опыт по результатам исследований и изучения возможностей управления информационной живучестью корабля, судна (ИЖС) как способности противостоять негативному воздействию на информационные системы и данные судна, сохраняя их целостность, доступность и конфиденциальность, несмотря на аварии, кибератаки и другие угрозы. Этот важный сегмент живучести судна предназначен для обеспечения безопасности экипажа, решения поставленных задач, живучести технических систем и сохранности груза. В контексте требований НБЖ-ТС-2002 приведены способы и средства обеспечения ИЖС, включая сравнительную оценку альтернативных вариантов.

**Ключевые слова:** борьба за живучесть корабля, судна; информационная живучесть судна; автоматизация процессов борьбы за ИЖС; защищенное исполнение; цифровая модель; система комплексной защиты информации; качество; эффективность; роботизация управления ИЖС.

### INFORMATIONAL SURVIVABILITY OF A SHIP: A MASTER CLASS

Alekseev Anatoly

Institute for Automation of Ship and Vessel Damage Control Processes  
101 Leninsky Av., of. 162, 198262, Saint Petersburg, Russia  
e-mail: [lapbgks@bk.ru](mailto:lapbgks@bk.ru)

**Abstract.** In the format of a master class on the automation of the processes of fighting for the survivability of a ship, the accumulated knowledge and practical experience on new research results and the study of the possibilities of managing the information survivability of a ship are summarized and presented as an ability to withstand the negative impact on the ship's information systems and data, while maintaining their integrity, accessibility and confidentiality, despite accidents, cyber attacks and other threats. This important segment of the ship's survivability is designed to ensure the safety of the crew, the solution of tasks, the survivability of technical systems and the safety of cargo. In the context of the requirements of NBZH-TS-2002, the methods and means of providing residential housing, including a comparative assessment of alternative options, are given.

**Keywords:** the struggle for the survivability of a ship, vessel; information survivability of a vessel; automation of the processes of fighting for residential housing; secure execution; digital model; integrated information protection system; quality; efficiency; robotization of residential housing management.

Накопленный опыт исследования технологий автоматизации процессов борьбы за живучесть корабля, судна (АП БЖКС), ранее обобщенный в коллективной монографии [1], сегодня требует учета и его расширения, прежде всего, в части введения нового понятия ИЖС [2, 3] и результатов обобщения уже выполненных исследований, включая [4-6] в сравнении с [7-12], требованиями [13-14] в контексте [15-22].

В формате мастер-класса по тематике автоматизации процессов борьбы за живучесть корабля, судна, включая требования НБЖ-ТС-2002 [13-14], впервые обобщены и представлены накопленные знания и практический опыт по результатам исследований и изучения возможностей управления информационной живучестью корабля, судна как способности противостоять негативному воздействию на информационные

системы и данные судна, сохраняя их целостность, доступность и конфиденциальность, несмотря на аварии, кибератаки и другие угрозы. Этот важный сегмент живучести судна предназначен для обеспечения безопасности экипажа, безопасности управления кораблем, судном, гарантированного решения поставленных задач, обеспечения живучести технических систем и оружия для кораблей, сохранности груза.

В контексте требований НБЖ-ТС-2002 [14] и ГОСТ Р 56024-2014 [13] приведены способы и средства обеспечения ИЖС, включая сравнительную оценку альтернативных вариантов средств и систем типа:

- систем информационной поддержки принятия решений при БЖКС (СИП);
- систем поддержки принятия решений и управления объектами информатизации (СПРУ);
- систем организационно-технического мониторинга и управления объектами (СОТМУ);
- интеллектуальных и роботизированных СПРУ (ИСПРУ) сложными объектами;
- роботизированных проектных полимодельных комплексов цифровых двойников (ЦД) управления

БЖКС, включая выделенный сегмент управления ИЖС (РПК ЦД);

- распределенных систем управления БЖКС, включая контур управления ИЖС (РСУ БЖКСиж).

В формате мастер-класса в структурированном виде представлены и проанализированы вопросы:

— исторические аспекты информационного противоборства и формирование систем понятий в области информационной безопасности и информационного противодействия [4, 5];

- 21 пример лучших практик информационной разведки, вторжений и противодействия [6];
- квалиметрическая парадигма интегральной оценки качества сложных систем [7];
- теоретические основы и проблемы информационной безопасности объектов информатизации;
- системные критерии и показатели оценки свойств и характеристик типовой СКЗИ;
- полимодельная парадигма аддитивности качества, его оценки, модели А.Н. Крылова и Ф. Нэша;
- аналитическая модель оценки качества СКЗИ и ее компьютерная реализация [6, 17-19, 22];
- теория анализа, синтеза и оптимизации СКЗИ АСЗИ в составе ОМТИ [6, 16];
- оценка и использование индексов корневой чувствительности при оптимизации СКЗИ [6, 17];
- ранжирование показателей конкурентной способности и перспективности развития АСЗИ [21];
- проблема цифровизации конфиденциальности, доступности, целостности [17];
- свойства и характеристики средств и систем комплексной защиты информации (СКЗИ);
- 4700 средств и систем защиты информации, возможности, свойства, характеристики;
- практика сертификации средств и систем защиты информации [18];
- парадигма инструментальной оценки качества и сертификации СКЗИ [19, 20];
- прикладная теория систем комплексной защиты информации; структура и приложения [6];
- практика проектирования и оптимизации СКЗИ в составе АСЗИ [21, 22];
- структура, возможности, свойства и характеристики калькулятора ИБ типа РПК «КАСОР-23»;
- технология цифрового двойника ИБ на базе РПК «КСР-24» и их систем.

Систематизация полученных и представленных теоретических и практических данных в форме мастер-класса с их фиксацией в соответствующих базах данных и знаний типа РПК «КАСОР-25.ИЖС» позволяет авторам — аккумулировать, апробировать и непрерывно актуализировать с участием научно-технического сообщества научно-технологический потенциал, а сообществу — обмениваться передовыми взглядами и результатами исследований в предметной области информационной живучести корабля, судна. В свою очередь, обществу — обоснованно выходить на конкурентно способные системные и организационно-технологические решения при одновременной и существенной экономии ресурсных затрат, аргументированно решать задачи инновационного развития и инвестиционного обоснования.

## СПИСОК ЛИТЕРАТУРЫ

1. Автоматизация процессов борьбы за живучесть корабля, судна// Коллективная монография Санкт-Петербург: ИАП БЖКС, эл. интерактивное изд. (третье), испр. и доп., с приложением, 2022. 506 с.
2. Субетто А.И., Алексеев А.В. Теория практики квалиметрического обеспечения развития морских автоматизированных систем / Актуальные проблемы морской энергетики: материалы седьмой Всероссийской межотраслевой научно-технической конференции в рамках Второго ВНТФ «Корабельная энергетика: из прошлого в будущее». СПб.: Изд-во СПбГМТУ, 2018, с. 78-86.
3. Алексеев А.В. Информационная живучесть судна: понятие, проблемы, технологии / Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 7 / СПОИСУ. СПб., 2019, с. 345-348.
4. Алексеев А.В., Воробьев В.И. Информационное противоборство: 20 лет концептуального и технологического развития // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 1 / СПОИСУ. СПб., 2015, с. 153-159.
5. Алексеев А.В. 30 лет концептуального и технологического развития проблем информационного противоборства / Труды Санкт-Петербургского государственного морского технического университета (СПбГМТУ). Выпуск 5 (9), 2025, с. 5-14.
6. Алексеев А.В. Прикладная теория информационной безопасности: структура, основные положения и приложения / Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 13 / СПОИСУ. СПб., 2024, 415-420.
7. Бобрович В.Ю., Алексеев А.В., Антипов В.В., Смольников А.В. Информационная живучесть корабля: угрозы, модель, системные требования, пути реализации / Информационная безопасность регионов России (ИБРР-2021). СПб., 2021, с. 265-267.
8. Robert J. Ellison, David A. Fisher, Richard C. Linger, Howard F. Lipson, Thomas A. Longstaff, Nancy R. Mead "Survivable Network Systems: An Emerging Discipline" // <http://www.cert.org/research/97tr013.pdf>
9. Robert J. Ellison, David A. Fisher, Richard C. Linger, Howard F. Lipson, Thomas A. Longstaff, Nancy R. Mead "Survivability: Protecting Your Critical Systems" // <http://www.cert.org/archive/html/protect-critical-systems.htm>
10. Додонов А.Г., Горбачик Е.С., Кузнецова М.Г. Живучесть компьютерных систем и безопасность информационной инфраструктуры // <https://cyberleninka.ru/article/n/zhivuchest-kompyuternyh-sistem-i-bezopasnost-informatsionnoy-infrastruktury/viewer/>
11. Максимов Р.В., Савинов Е.А. Оценка живучести распределенных интегрированных информационных систем / Информационные технологии и нанотехнологии, 2016.
12. Громов Ю.Ю., Винокуров Д.Е., Самхарадзе Т.Г. Пасечников И.И. Анализ живучести информационных сетей / Информационные процессы и управление, 2006, № 1, с. 138-154.
13. ГОСТ Р 56024— 2014. Система управления безопасностью судов. Требования к организации обеспечения живучести судна, 2014.- 36с.

14. Наставление по борьбе за живучесть морских (речных) таможенных судов Российской Федерации (НБЖ-ТС-2002).
15. Максимова М.А., Согонов С.А., Михальчук А.В. Модель и технология цифровых двойников систем автоматизации судов / Труды Санкт-Петербургского государственного морского технического университета (СПбГМТУ). Выпуск 4 (8), 2023, с. 5-14.
16. Алексеев А.В. Информационная живучесть управления: теория и практика обеспечения информационного превосходства / Информационная безопасность регионов России (ИБРР-2023). XIII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 25-27 октября 2023 г.: Материалы конференции / СПОИСУ. СПб, 2023, с. 224-226.
17. Алексеев А.В., Михальчук А.В. Цифровой двойник системы комплексной защиты информации в инвариантном исполнении (ИД СКЗИ) / Свидетельство о государственной регистрации программ для ЭВМ (Реестр ФСИС) № 2014613622, 01.04.2023 (06.02.2014).
18. Корнева Ю.В., Алексеев А.В. Информационная живучесть тактической группы кораблей. СПбГМТУ: ВКР, 2023, 75 с.
19. Алексеев А.В., Михальчук А.В. Цифровой мониторинг, прогнозирование и контроль успешности реализации комплекса организационно-технических решений (ЦМПК, цифровой двойник) / Свидетельство о государственной регистрации программ для ЭВМ (Реестр программ Федеральной службы по интеллектуальной собственности) № 2023661669, 01.06.2023.
20. Алексеев А.В., Антипов В.В., Смольников А.В. Сертификация качества моделей на примере цифровых двойников управления борьбой за живучесть корабля, судна / Труды СПбГМТУ. Выпуск 5 (9), 2025, с. 5-14.
21. Алексеев А.В., Согонов С.А., Михальчук А.В. Цифровые тренды развития морских интегрированных систем управления в защищенном исполнении: теория практики интеллектуализации и роботизации / Материалы Форума АЗИ «Актуальные вопросы информационной безопасности» и VI Всероссийской научно-практической конференции с международным участием «Цифровая трансформация науки и образования». М.: АЗИ, 2025, с. 47-57.
22. Алексеев А.В., Дригола В.К., Михальчук А.В. Информационная живучесть корабля, судна: прикладная теория обеспечения военно-технологического превосходства / Телекоммуникации и связь. Научный рецензируемый журнал. 2025, № 4 (07), с. 79-87.

УДК 004.05

## К ВОПРОСУ О РАЗРАБОТКЕ СИСТЕМЫ ДЛЯ ЭФФЕКТИВНОГО И ОБЪЕКТИВНОГО РАНЖИРОВАНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Богатырёв Данил Вячеславович

Санкт-Петербургский государственный морской технический университет

Лоцманская ул., 3, Санкт-Петербург, 190121, Россия

e-mail: bogatyrov\_d@mail.ru

**Аннотация.** Рассматривается вопрос об общем принципе построения и возможных направлениях развития комплексных автоматизированных систем оценки и выбора программных решений для обеспечения информационной безопасности объекта. Показано, что предлагаемый подход, лежащий в основе системы “КАСОР”, позволяет на основе цифровых показателей эффективности объективно ранжировать и выбирать наиболее подходящие средства защиты информации для конкретной инфраструктуры и угроз. Может использоваться при проектировании и внедрении комплексных систем информационной безопасности, а также для оптимизации существующих систем защиты на основе анализа их фактической эффективности. Перспективно для развития и модернизации средств обеспечения информационной безопасности объектов различного масштаба и назначения.

**Ключевые слова:** автоматизированная система; оценка; выбор; программные решения; информационная безопасность; объект; цифровые показатели; эффективность; ранжирование; средства защиты информации; инфраструктура; угрозы; проектирование; внедрение; оптимизация; развитие; модернизация.

## ON THE ISSUE OF DEVELOPING A SYSTEM FOR EFFECTIVE AND OBJECTIVE RANKING OF INFORMATION SECURITY TOOLS

Bogatyrev Danil

Saint Petersburg State Marine Technical University

3 Lotsmanskaya St., Saint Petersburg, 190121, Russia

e-mail: bogatyrov\_d@mail.ru

**Abstract.** This paper explores the design and development of automated systems for evaluating and selecting cybersecurity software. It demonstrates that “KASOR” leverages digital performance indicators to objectively rank and choose optimal security solutions tailored to specific infrastructure and threats, promising enhanced information security for organizations of all sizes.

**Keywords:** automated system; evaluation; selection; software solutions; information security; object; digital indicators; efficiency; ranking; information security tools; infrastructure; threats; design; implementation; optimization; development; modernization.

Система информационной безопасности объекта, как основной гарант защиты данных, является системой первого порядка в более сложной системе — организации. Поэтому требования к системе информационной безопасности в части надёжности и эффективности очень высоки, вследствие ее основного функционального назначения. Нарушение работоспособности системы информационной безопасности может привести к утечке конфиденциальной информации, финансовым потерям, репутационным рискам, и в конечном счете, к срыву выполнения организацией поставленных задач, а в случае возникновения инцидента — и к тяжелым последствиям.

Надёжность системы информационной безопасности в целом, и комплектующих ее программных и аппаратных средств (средств защиты информации, СЗИ), в частности, должна обеспечиваться соответствующими архитектурными решениями, принятой политикой безопасности, соблюдением инструкций

по эксплуатации, мониторингом текущего состояния защиты, технологиями обновления, аудита и управления инцидентами [1].

С точки зрения системного подхода, система информационной безопасности относится к классу сложных технических комплексов с динамической структурой. Связи и свойства ее компонентов (СЗИ) изменяются в течение всего периода эксплуатации, адаптируясь к новым угрозам и изменяющимся требованиям. Вместе с тем, как правило, качество функционирования таких комплексов со временем ухудшается из-за появления новых уязвимостей и более совершенных методов атак. Восстановительные мероприятия, проводимые в рамках системы аудита, реагирования на инциденты и обновления, лишь частично снижают темп деградации уровня защиты.

В этой связи, в процессе эксплуатации особо важная роль отводится непрерывному мониторингу и оценке эффективности отдельных СЗИ, способных лимитировать общий уровень защиты. Под мониторингом и оценкой в данном контексте понимается взаимоувязанная последовательность выполнения следующих процедур: сбор и анализ данных о функционировании СЗИ, их эффективности в отражении атак, соответствии настройкам и политикам; обработка и анализ результатов измерений с выдачей заключения о степени соответствия требованиям безопасности; прогноз эффективности СЗИ в будущем с учетом меняющегося ландшафта угроз и выдача рекомендаций специалистам по информационной безопасности. Реализация указанных процедур предполагает наличие автоматизированной системы комплексной оценки и выбора СЗИ, такой как "КАСОР" [2, 3].

Необходимость наличия подобных систем оценки и выбора СЗИ подтверждается тем, что во многих организациях отсутствует, в необходимом объеме, система мониторинга (или экспертная система), направленная на индикацию и прогнозирование эффективности используемых средств защиты информации. Кроме того, наблюдается недостаточная инициатива отечественных фирм по использованию систем оценки и выбора СЗИ, которые могут быть реализованы в виде одной из функций локальной или комплексной системы контроля за средствами защиты информации.

#### СПИСОК ЛИТЕРАТУРЫ

1. Василенко, В. А. Мониторинг технического состояния корабельных ядерных энергетических установок / В. А. Василенко, С. Я. Травин. Санкт-Петербург: Моринтех, 2006. 256 с.
2. Баканов, В. Н. Состояние и проблемы автоматизации надводных кораблей / В. Н. Баканов. Санкт-Петербург: ОАО «Концерн НПО «Аврора», 2009. 142 с.
3. Мониторинг технического состояния корабельного энергетического оборудования [Электронный ресурс]. URL: <https://spravochnik.ru/lektoriy/monitoring-tehnicheskogo-sostoyaniya-korabelnogo-energeticheskogo-oborudovaniya/> (дата обращения: 15.08.2025).

УДК 004.056.5

#### ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ

Вареница Лидия Андреевна

Санкт-Петербургский государственный морской технический университет

Лоцманская ул., 3, Санкт-Петербург, 190121, Россия

e-mail: lidiya.voenitsa@email.com

**Аннотация.** В статье исследуются методы обеспечения кибербезопасности систем управления технологическими процессами (АСУ ТП) на промышленных предприятиях. Рассмотрены уязвимости, специфичные для АСУ ТП, а также подходы к их выявлению и устранению. Анализируются современные методы защиты, такие как сегментация сети, системы обнаружения вторжений (IDS) и механизмы контроля целостности программного обеспечения. Особое внимание уделено защите от целенаправленных атак и обеспечению отказоустойчивости критически важных компонентов АСУ ТП.

**Ключевые слова:** АСУ ТП; кибербезопасность; промышленная безопасность; уязвимости; обнаружение вторжений; отказоустойчивость; сегментация сети.

#### ENSURING CYBERSECURITY OF INDUSTRIAL CONTROL SYSTEMS

Varenitsa Lidia

Saint Petersburg State Marine Technical University

3 Lotsmanskaya St., Saint Petersburg, 190121, Russia

e-mail: lidiya.voenitsa@email.com

**Abstract.** The article examines methods for ensuring the cybersecurity of industrial control systems (ICS) in industrial enterprises. Vulnerabilities specific to ICS, as well as approaches to their identification and elimination, are considered. Modern protection methods such as network segmentation, intrusion detection systems (IDS), and software integrity control mechanisms are analyzed. Particular attention is paid to protection against targeted attacks and ensuring the resilience of critical ICS components.

**Keywords:** ICS; cybersecurity; industrial security; vulnerabilities; intrusion detection; resilience; network segmentation.

Современные целенаправленные атаки представляют собой одну из наиболее серьезных угроз для систем управления технологическими процессами (АСУ ТП) на промышленных предприятиях, включая энергетику, химическую промышленность и транспорт. С цифровизацией производства и расширением сетевой взаимосвязанности АСУ ТП, уязвимости и потенциальные векторы атак неуклонно растут. Это требует разработки адаптивных систем защиты, способных противостоять как известным, так и новым формам кибервторжений.

Основной задачей при обеспечении кибербезопасности АСУ ТП является обнаружение и предотвращение несанкционированного доступа, а также манипуляций с данными и оборудованием. Для этого применяются многоуровневые системы защиты, включающие физическую безопасность, контроль доступа, мониторинг сетевой активности и анализ программного обеспечения. Особое внимание уделяется выявлению и устранению уязвимостей в программном обеспечении АСУ ТП, а также защите от вредоносного кода [1-3].

Эффективным подходом является сегментация сети АСУ ТП, т.е. разделение ее на отдельные зоны с различными уровнями доступа и контроля. Это позволяет ограничить распространение вредоносного программного обеспечения и предотвратить масштабные аварии в случае компрометации одного из сегментов. Кроме того, важным является использование специализированных систем обнаружения вторжений (IDS) и систем предотвращения вторжений (IPS), адаптированных для протоколов и особенностей АСУ ТП.

Для защиты критически важных объектов АСУ ТП все чаще применяется:

- Резервирование оборудования и каналов связи;
- Реализация механизмов отказоустойчивости и автоматического переключения на резервные системы;
- Использование двухфакторной аутентификации для доступа к критическим функциям;
- Регулярное обновление программного обеспечения и устранение уязвимостей.

Важным направлением является разработка интеллектуальных систем мониторинга и диагностики на основе машинного обучения. Алгоритмы машинного обучения позволяют выявлять аномалии в работе оборудования и сетевой активности, сигнализируя о возможных кибератаках или сбоях в работе АСУ ТП [4-7].

Особую сложность представляет защита от атак, направленных на нарушение целостности данных и изменение логики работы АСУ ТП. Для противодействия таким угрозам применяются:

- Цифровые подписи для защиты критически важных файлов и конфигураций;
- Механизмы контроля целостности программного обеспечения;
- Использование криптографических методов для защиты данных, передаваемых между компонентами АСУ ТП.

В системах управления критической инфраструктурой дополнительную сложность создает требование обеспечения непрерывности технологического процесса. Это требует разработки отказоустойчивых и самовосстанавливающихся систем защиты, способных минимизировать влияние кибератак на работу АСУ ТП.

Перспективным направлением является разработка платформ обмена информацией об угрозах в сфере промышленной кибербезопасности. Это позволит оперативно обмениваться данными об уязвимостях, атаках и методах защиты, повышая общий уровень защищенности АСУ ТП.

Таким образом, современные системы обеспечения кибербезопасности АСУ ТП должны сочетать многоуровневый подход, включающий как проверенные методы защиты периметра, так и интеллектуальные технологии анализа аномалий и реагирования на инциденты, обеспечивая при этом непрерывность и надежность технологического процесса.

#### СПИСОК ЛИТЕРАТУРЫ

1. Зайцев А. В. Кибербезопасность промышленных систем управления. М.: Лаборатория знаний, 2020. 420 с.
2. Humayed A., Lin J., Li F., Buyya R. A Survey of Cyber Security Threats and Solutions in Industrial Control Systems. IEEE Transactions on Industrial Informatics, 2017.
3. Stouffer K., Falco J., Scarfone K. Guide to Industrial Control Systems (ICS) Security. NIST Special Publication 800-82, 2015.
4. Бердичевский В.Ю., Кузнецов С.О. Моделирование угроз безопасности АСУ ТП. М.: Инфра-М, 2018. 192 с.
5. Олейник А.С., Романова Ю.Д. Анализ уязвимостей и методы защиты АСУ ТП. СПб.: Лань, 2021. 288 с.
6. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). Alerts and Advisories. [Электронный ресурс]. URL: [https://itlaw.fandom.com/wiki/Industrial\\_Control\\_Systems\\_Cyber\\_Emergency\\_Response\\_Team](https://itlaw.fandom.com/wiki/Industrial_Control_Systems_Cyber_Emergency_Response_Team) (дата обращения: 02.08.2025).
7. SANS Institute. Industrial Control System Security Resources. 2023. [Электронный ресурс]. URL: <https://rmcglobal.com/wp-content/uploads/2023/09/SANS-2023-ICS-OT-Cybersecurity-Survey-Results-White-Paper-RMC.pdf> (дата обращения: 01.08.2025).

УДК 681.3.06

#### ИНТЕГРАЦИЯ CNC-ТЕХНОЛОГИЙ В ЦИФРОВУЮ ЭКОСИСТЕМУ СУДОСТРОЕНИЯ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

**Васюкова Мария Сергеевна**

Санкт-Петербургский государственный морской технический университет  
Лоцманская ул., 3, Санкт-Петербург, 190121, Россия  
e-mail: 79061334506@yandex.ru

**Аннотация.** В тезисах рассматривается процесс интеграции современных CNC-систем в цифровую экосистему судостроительного предприятия в информационно-защищенном исполнении на примере АО «Адмиралтейские верфи». Обоснована необходимость актуализации базы знаний ИТ-класса CNC, оценены

программные решения и проведена апробация с использованием симулятора FANUC. Представлена методика создания цифрового двойника производственного участка с применением программного комплекса «КСР-25». Выделены ключевые направления цифровизации судостроения, включая повышение точности, обеспечение информационной защищенности, снижение затрат и обеспечение технологического суверенитета. Сделан вывод о перспективности внедрения гибридных ИТ-решений на основе импортных и отечественных разработок с условием обеспечения гарантированной защиты данных.

**Ключевые слова:** CNC; цифровая экосистема; цифровой двойник; база знаний; FANUC; ЧПУ; судостроение; КСР-25; информационно-защищенное исполнение.

## INTEGRATION OF CNC TECHNOLOGIES INTO THE DIGITAL ECOSYSTEM OF SHIPBUILDING IN A SECURE DESIGN

Vasyukova Maria

Saint Petersburg State Marine Technical University  
3 Lotsmanskaya St., Saint Petersburg, 190121, Russia  
e-mail: 79061334506@yandex.ru

**Abstract.** The theses consider the process of integrating modern CNC systems into the digital ecosystem of a shipbuilding enterprise in an information-secure design using the example of Admiralty Shipyards JSC. The necessity of updating the knowledge base of the CNC IT class is substantiated, software solutions are evaluated and tested using the FANUC simulator. A technique for creating a digital twin of a production site using the KSPR-25 software package is presented. The key areas of digitalization of shipbuilding are highlighted, including improving accuracy, ensuring information security, reducing costs and ensuring technological sovereignty. The conclusion is made about the prospects of introducing hybrid IT solutions based on imported and domestic developments with the condition of ensuring guaranteed data protection.

**Keywords:** CNC; digital ecosystem; digital twin; knowledge base; FANUC; numerical control; shipbuilding; KSPR-25; information-protected execution.

В условиях стремительного перехода промышленности к концепции индустрии 4.0 особую актуальность приобретает интеграция высокоточных цифровых систем управления в общую информационную инфраструктуру предприятия. Одной из таких систем являются CNC-технологии (Computer Numerical Control), обеспечивающие автоматизированное управление оборудованием на всех этапах жизненного цикла морской техники. Данный подход особенно важен для судостроительной отрасли, где требования к точности, информационной защищенности, срокам и качеству исполнения находятся на пределе технологических возможностей.

Целью настоящей работы является анализ и апробация подходов к интеграции CNC-технологий в цифровую экосистему АО «Адмиралтейские верфи» в защищенном исполнении с последующим созданием цифрового двойника (ЦД) производственного процесса. Основное внимание уделено актуализации базы данных и знаний (БДЗ) CNC-класса ИТ, оценке программных решений и разработке адаптивной цифровой модели управления [1].

На первом этапе был проведен комплексный анализ современных CNC-систем с точки зрения их соответствия требованиям судостроительного производства, включая оценку устойчивости к внешним угрозам и защиты критически важных данных от несанкционированного доступа. Рассматривались такие параметры, как точность обработки, поддержка многоосевой обработки, совместимость с CAD/CAM-средами, возможность встраивания в корпоративную информационную среду (MES/ERP) и требования по защите информации. Среди наиболее подходящих решений выделены Siemens Sinumerik, Fanuc CNC и отечественные разработки (SprutCAM, LinuxCNC). Были также изучены вопросы импортозамещения и перехода к гибридным архитектурам.

Проведена практическая апробация CNC-решения на базе ПО SwanSoft FANUC CNC Simulator. Данное программное обеспечение позволяет в полной мере моделировать работу станков с ЧПУ без необходимости физического доступа к оборудованию. В ходе апробации было продемонстрировано фрезерование и токарная обработка деталей, выполнен анализ структуры управляющих программ, режимов AUTO и EDIT, а также визуализация траекторий инструмента. Полученные результаты подтвердили эффективность применения симуляторов для подготовки персонала и оптимизации производственных процессов, а также продемонстрировали их потенциал в области обеспечения безопасности информации.

Следующим этапом стало построение цифрового двойника производственного участка с применением данных о CNC-системах, технологических операциях, параметрах обработки и степени защищенности предприятия от внешних и внутренних угроз. В качестве базовой платформы использовался программный комплекс «КСР-25», который обеспечил интеграцию производственных сценариев, мониторинг состояния оборудования и анализ эффективности. Такой подход позволил моделировать изменения в технологии, оценивать влияние режимов резания на ресурсоёмкость операций и выявлять узкие места в производственной цепочке.

На основе проведенного анализа и моделирования была разработана методика интеграции CNC-систем в защищенном исполнении в цифровую экосистему предприятия. Ключевыми компонентами этой методики стали: унификация баз данных CNC-оборудования, автоматизация обмена данными с CAD/CAM-системами, внедрение

аналитических модулей на основе ISO/G-кодов и построение гибкой архитектуры ЦД с возможностью масштабирования [2, 3].

Интеграция CNC-технологий в цифровую экосистему судостроения в защищенном исполнении позволяет добиться синергии между автоматизированными производственными системами, интеллектуальной обработкой данных и гибким управлением ресурсами. Это формирует основу для перехода к новым моделям цифрового производства, повышения технологической независимости и конкурентоспособности отечественных верфей. Полученные результаты подтверждают актуальность и перспективность дальнейшего развития цифровых двойников на базе CNC и других интеллектуальных систем в отрасли морского машиностроения [4].

#### СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 55842-2019. Системы числового программного управления. Требования безопасности и методы испытаний. М.: Стандартинформ, 2019.
2. Иванов, К. Л. Разработка методов адаптивного управления CNC-системами в условиях цифрового производства / К. Л. Иванов. СПб., 2021. 145 с.
3. Петров, И. С. Современные тенденции развития CNC-систем в судостроении / И. С. Петров, О. Н. Васильева // Судостроение. 2022. № 4. С. 15–22.
4. Смирнов, А. В. Числовое программное управление станками / А. В. Смирнов, В. Г. Козлов. СПб.: Политехника, 2020. 320 с.

УДК 004.9

### **К ВОПРОСУ О ПРАКТИЧЕСКОМ ОСВОЕНИИ СИСТЕМЫ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ «САПР» В ЦЕНТРЕ СУДОРЕМОНТА АО «ЦС «ЗВЕЗДОЧКА» С ПРИМЕНЕНИЕМ КВАЛИМЕТРИЧЕСКОГО РАНЖИРОВАНИЯ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ**

**Верещагин Анатолий Васильевич**

Санкт-Петербургский государственный морской технический университет  
Лотманская ул., 3, Санкт-Петербург, 190121, Россия  
e-mail: vereshagin-apostol@yandex.ru

**Аннотация.** Рассматривается вопрос освоения системы автоматизированного проектирования «САПР» AutomatiCS в центр судоремонта АО «ЦС «Звездочка» с использованием квалиметрического ранжирования, включая оценку соответствия системы требованиям информационной безопасности.

**Ключевые слова:** система автоматизированного проектирования САПР; квалиметрическое ранжирование; критерии сравнения; агрегированный показатель качества; AutomatiCS; конкурентоспособность; программный комплекс «КСР»; защищенное исполнение.

### **ON THE PRACTICAL DEVELOPMENT OF A CAD SYSTEM AT THE SHIP REPAIR CENTER OF JSC «CS» «ZVEZDOCHKA», USING QUALITY RANKING IN A PROTECTED EXECUTION**

**Vereshchagin Anatoly**

Saint Petersburg State Maritime Technical University  
3 Lotsmanskaya St., Saint Petersburg, 190121, Russia  
e-mail: vereshagin-apostol@yandex.ru

В промышленном производстве давно царит жесткая конкуренция. Чтобы выжить в этих нелегких условиях, предприятиям приходится как можно быстрее выпускать новые изделия, снижать их себестоимость и повышать качество. В этом им помогают современные CAD/CAM/CAE-системы (САПР), позволяющие облегчить весь цикл разработки изделий — от выработки концепции до создания опытного образца и запуска его в производство, гарантируя надежную защиту проектных данных на всех этапах жизненного цикла изделия. Тем самым значительно ускоряется процесс создания новой продукции без ущерба качеству. Поэтому сейчас без САПР не обходится ни одно конструкторское или промышленное предприятие.

Система автоматизированного проектирования (САПР) — автоматизированная система, реализующая информационную технологию выполнения функций проектирования, представляющая собой организационно-техническую систему, предназначенную для автоматизации процесса проектирования, состоящую из персонала и комплекса технических, программных и других средств автоматизации его деятельности.

Освоение САПР — серьезное научно-практическое мероприятие, требующее немалых инвестиций. Цель его — максимально использовать возможности программного обеспечения при решении различных задач предприятия [1].

В настоящее время качество продукции стало определяющим фактором конкурентной борьбы на рынке. Оно должно быть обеспечено на всех этапах периода существования изделия. Важную роль в задачах обеспечения качества играет квалиметрия — область знания, посвященная методам получения количественных оценок качества объектов, используемых человеком, независимо от их природы.

Целью самостоятельной работы является определение лучших информационных технологий класса САПР и выявление лучших практик их освоения применительно к электромеханическим цехам, а именно: цех ремонта корабельного оборудования; цех ремонта и испытаний корабельных систем; цехи ремонта судовой и корабельной



электроаппаратуры с учетом требований информационной безопасности к защите проектных данных, контролю доступа к производственной документации и предотвращению несанкционированного вмешательства в производственные процессы [2].

Для достижения цели самостоятельной работы, а именно квалиметрического ранжирования ИТ систем САПР и практик их применения, предусматривается решение следующих задач:

- Выявление особенностей практик применения ИТ систем САПР в производственных мощностях АО «ЦС «Звездочка», задействованных в модернизации и ремонте заказов;
- Оценка соответствия ИТ класса требованиям к проектируемым и модернизируемым заказам;
- Автоматизированное планирование выполнения СР с применением программного комплекса (далее ПК) «Прогноз»;
- Формирование базы данных ИТ системы САПР. Формирование критериев оценки качества, исследуемых ИТ. Квалиметрическое ранжирование ИТ ЗК и анализ полученных результатов (с применением ПК «АСОР»);
- Разработка перечня лучших практик освоения ИТ класса САПР;
- Апробация ИТ класса САПР при управлении ЖЦ ОМИ типа АО «ЦС «Звездочка». Выявления, по результатам апробации, свойств и особенностей ИТ;
- Выдвижение предложений по цифровой трансформации ОМИ ЗК;
- Выдвижение предложений по обеспечению безопасности САПР-систем на всех этапах жизненного цикла.

Правильно выполненное освоение САПР весьма продуктивно работает на развитие и совершенствование проектно-конструкторской деятельности и всего предприятия в целом.

Анализ состояния и проблем развития ИТ в классе систем автоматизированного проектирования САПР позволяет оценить текущее положение этой области и выявить проблемы, с которыми она сталкивается, а также определить лучшие практики для их решения и освоения.

САПР продолжает развиваться, внедряя новые технологии, такие как трехмерное моделирование, виртуальная реальность, облачные вычисления и искусственный интеллект, что позволяет повышать эффективность и точность проектирования. При этом особое внимание уделяется вопросам информационной безопасности: используются методы шифрования данных, многофакторная аутентификация, защищенные облачные хранилища и системы мониторинга киберугроз.

САПР становится все более интегрированным с другими информационными системами в предприятии, такими как системы управления жизненным циклом продукта (PLM), управления предприятием (ERP) и управления отношениями с клиентами [3].

Целью самостоятельной работы была разработка критериев сравнения и рекомендации по выбору систем автоматизированного проектирования в защищенном исполнении. Для выявления систем автоматизированного проектирования в наибольшей степени, удовлетворяющей конкретным запросам пользователей, был проведен сравнительный анализ этих систем.

В ходе исследования систем автоматизированного проектирования для освоения систем автоматизированного проектирования (САПР) в производственные процессы АО ЦО «Звездочка» в защищенном исполнении был использован программный комплекс «КСРП», разработанный в СПбГМТУ в рамках разнородных исследований с учетом специфических производственных особенностей АО «ЦО «Звездочка».

В ходе работы была разработана система критериев для адекватной оценки и сравнения систем автоматического проектирования САПР с использованием метода квалиметрического ранжирования и оптимизации выбора информационных систем в классе СРС. При выборе системы был учтен критерий максимума агрегированного показателя качества с учетом специфики АО «ЦО «Звездочка».

После числового моделирования и многовариантного анализа различных систем САПР был обоснован выбор лидеров рынка. Также были определены преимущества и недостатки этих лидеров для их дальнейшего развития.

#### СПИСОК ЛИТЕРАТУРЫ

1. Петухов, А. В. Системы автоматизированного проектирования технологических процессов / А. В. Петухов, Д. В. Мельников, В. М. Быстренков. Гомель, 2011.
2. САПР инструментарий проектировщика в XXI веке Ремир Сольницев Д.т.н., профессор кафедры САПР СПбГЭТУ «ЛЭТИ».
3. Нестеренко, Е. С. Основы систем автоматизированного проектирования / Е. С. Нестеренко, 2024.

УДК 004.056.5

### ОЦЕНКА ИСПОЛЬЗОВАНИЯ «РПК-КАСОР 23.5» В ОБЛАСТИ ЗАЩИТЫ ОБЪЕКТОВ МОРСКОЙ ИНФРАСТРУКТУРЫ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

**Вчерашний Михаил Павлович**

Санкт-Петербургский государственный морской технический университет

Лоцманская ул., 3, Санкт-Петербург, 190121, Россия

e-mail: mikhael.vcherashniy@mail.ru

**Аннотация.** Рассматривается оценка использования технологии «РПК «КАСОР-23.5» в области защиты объектов морской инфраструктуры а информационно защищенном исполнении (ОМИзи). Оценены возможности технологии КАСОР по обеспечению защиты информационных ресурсов ОМИзи. Рассмотрены технологии защиты ОМИзи, включая защиту персональных данных, особенности критической информационной инфраструктуры. Дан ответ на вопрос о достаточности применения только этой технологии или понадобятся ещё инструменты и технические средства для защиты ОМИзи.

**Ключевые слова:** технология; защита; безопасность; морская инфраструктура; проектное качество; эффективность; валидация.

## EVALUATION OF THE USE OF PKK-KASOR 23.5 IN THE FIELD OF PROTECTION OF MARINE INFRASTRUCTURE FACILITIES IN A SECURE DESIGN

Vcherashniy Mikhail

Saint Petersburg State Marine Technical University  
3 Lotsmanskaya St, Saint Petersburg, 190121, Russia  
e-mail: mikhail.vcherashniy@mail.ru

**Abstract.** The assessment of the use of PKK-KASOR 23.5 technology in the field of protection of information-protected marine infrastructure facilities (OMIzi) is being considered. The possibilities of the CASOR technology to ensure the protection of OMIzi information resources are evaluated. OMIzi protection technologies, including personal data protection, and features of critical information infrastructure are considered. The answer is given to the question of whether it is sufficient to use only this technology or whether more tools and technical means will be needed to protect OMIzi.

**Keywords:** technology; protection; safety; marine infrastructure; design quality; efficiency; validation.

Актуальность темы доклада состоит в том, что в настоящее время рынок IT-инфраструктуры крайне остро нуждается в отечественном решении. Причём не просто отечественном, а надёжным отечественном решении для объектов морской инфраструктуры.

Цель этого доклада состоит в оценке возможностей данной технологии и её эффективности в области защиты объекта морской инфраструктуры. Эта технология включает в себя множество аспектов, которые необходимо учитывать при построении защиты объекта в сфере информационной безопасности ОМИзи.

Одним из основных вопросов является адекватность выбранной для ранжирования средств и систем защиты информации на ОМИзи системы критериев для оценивания данной технологии, для чего необходимо:

Во-первых, разработать систему специфических для конкретного ОМИзи критериев оценивания рассматриваемой технологии, средств и систем комплексной защиты информации (СКЗИ).

Во-вторых, составить предметную дорожную карту для конкретных дальнейших шагов по использованию «РПК «КАСОР-23.5» при решении конкретных функциональных задач.

В-третьих, произвести практическое тестирование данной технологии на ОМИзи после проведения предварительного оценивания для учета корректности выбранной системы критериев, соответствующих показателей качества с учетом, а при возможности и минимизацией погрешностей оценивания.

В-четвертых, составить, апробировать (в научно-техническом сообществе) и утвердить уполномоченными лицами отчет об оценке результатов проведенных исследований и испытаний данной технологии на конкретном ОМИзи с указанием в нём полной и подробной информации о технологии и о методах её оценивания.

В-пятых, внести после утверждения в базу данных и знаний (БДЗ) роботизированного проектного комплекса «РПК «КАСОР-23.5» актуальные данные, включая новые и корректировку уже имеющихся данных.

Этот комплекс работ, предусмотренных в технологи квалитетического анализа, синтеза и оптимизации решений (КАСОР), разработанной в Санкт-Петербургском государственном морском техническом университете на Кафедре судовой автоматики и измерений [1], требует соответствующего ресурсного обеспечения для актуализации БДЗ, поддержания РПК «КАСОР-23.5» в актуальном состоянии по требованиям ФСТЭК РФ [2, 3].

В том числе для использования в составе средств инструментального аудита и контроля СКЗИ ОМИзи.

Перспективы внедрения данной технологии в этих условиях не вызывают сомнения, сегодня по существу являются безальтернативными, актуальными и особо востребованными, в том числе с учетом СВО. Могут быть и должны использоваться для цифровизации качества процессов создания, освоения и эксплуатации, а также средств и СКЗИ в составе автоматизированных систем при их сертификации, аттестации и аккредитации ОМИ.

## СПИСОК ЛИТЕРАТУРЫ

1. Алексеев А. В. Сертификация средств и систем защиты информации: конспект лекций / А. В. Алексеев ; СПбГМТУ, КСАиИ. СПб., 2023.
2. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации / Утверждено приказом ФСТЭК России от 25 декабря 2017 г. № 239.
3. Положение о системе сертификации средств защиты информации / Утверждено приказом ФСТЭК России от 3 апреля 2018 г. № 55.

УДК 004.05

**ЦИФРОВАЯ ОЦЕНКА КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ФЛОТИЛИЕЙ РАЗНОРОДНЫХ СИЛ****Дригола Владимир Кириллович<sup>1</sup>, Алексеев Анатолий Владимирович<sup>2</sup>**<sup>1</sup>Военный учебно-научный центр ВМФ «Военно-морская академия»

Ушаковская наб., д. 17/1, Санкт-Петербург, 197045, Россия

<sup>2</sup>Санкт-Петербургский государственный морской технический университет

Лоцманская ул., д.3, Санкт-Петербург, 199178, Россия

e-mails: velena.spb@mail.ru, lapbgks@bk.ru

**Аннотация.** Рассматривается задача компьютерного моделирования цифровой оценки комплексной защиты информации (КЗИ) распределенной системы управления (PCY) флотилией разнородных сил (ФлРС) на основе технологии квалиметрической оптимизации вариантного выбора. В состав системы критериев оценки проектного качества/эффективного функционирования PCY наряду с характерными критериями оценки качества систем управления ФлРС включены также критерии оценки их информационной живучести, включая групповые показатели военно-технического превосходства по КЗИ и по информационному противодействию (ИПД). Разработанная компьютерная модель и цифровая оценка КЗИ на базе роботизированного проектного комплекса (РПК) «КСР-2025» позволяет количественно обосновывать решения при проектировании главным конструктором, а также принимаемые командиром ФлРС (ЛПР) управленческие решения, выдавать рекомендации операторам пунктов управления при оптимизации управления по критерию максимизации военно-технического превосходства (ВТП) над противником.

**Ключевые слова:** распределенная система управления; комплексная защита информации; информационное противодействие; цифровая оценка и оптимизация качества управления.

**DIGITAL ASSESSMENT OF THE INTEGRATED INFORMATION PROTECTION OF A DISTRIBUTED FLOTILLA MANAGEMENT SYSTEM OF DIVERSE FORCES****Drigola Vladimir<sup>1</sup>, Alekseev Anatoly<sup>2</sup>**<sup>1</sup>Military Training and Research Center of the Navy «Naval Academy»

Ushakovskaya Embankment, 17/1, Saint Petersburg, 197045, Russia

<sup>2</sup>Sankt-St. Petersburg State Maritime Technical University

3 Lotsmanskaya St., St. Petersburg, 199178, Russia

e-mails: velena.spb@mail.ru, lapbgks@bk.ru

**Abstract.** The paper considers the problem of computer modeling of the digital assessment of integrated information security (CSI) of a distributed control system (DCS) for a flotilla of heterogeneous forces (FIRS) based on the technology of qualimetric optimization of variant selection. The system of criteria for evaluating the design quality/effective functioning of the DCS, along with the characteristic criteria for evaluating the quality of the control systems of the FIRS, also includes criteria for evaluating their information survivability, including group indicators of military-technical superiority in CSI and information counteraction (IPD). The developed computer model and digital assessment of the KPI based on the KSPR-2025 robotic design complex (PKK) allows quantifying design decisions by the chief designer, as well as management decisions made by the commander of the FIRS (LPR), and making recommendations to control point operators when optimizing management based on the criterion of maximizing military-technical superiority over the enemy.

**Keywords:** distributed management system; comprehensive information protection; information counteraction; digital assessment and optimization of management quality.

Одной из важнейших проблем в области информационной безопасности (ИБ) является моделирование процессов и цифровая оценка качества (при проектировании) и эффективности (при эксплуатации) систем комплексной защиты информации (СКЗИ) [1]. В настоящее время отсутствуют общепризнанные и адекватные модели и модельных исследований этих сложных и высоко динамичных процессов. Особую актуальность в связи с событиями СВО приобрели сегодня вопросы не только эффективного управления силами и оружием, но и задача обеспечения информационно-защищенного управления. Именно противоборство в информационной сфере сегодня является непрерывным по времени, пространству и диапазону используемых возможностей, в связи с чем, развитие PCY в информационно-защищенном исполнении (PCYзи) является одним из перспективных и высоко востребованных, так как обеспечивает из базовых требований наряду с непрерывностью управления его скрытность и устойчивость, а также, как следствие, оперативность управления [2 - 4]. Однако, для максимальной реализации этих возможностей, а, тем более, обеспечения военно-технического превосходства (ВТП) в управлении над противником (ВТПу) по этим критериям необходимо непрерывно развивать и иметь интеллектуальную подсистему (систему) поддержки решений и управления (ИСПРУ) силами и оружием в море и на берегу, включая факторы и параметры СКЗИ.

Технологической основой таких ИСПРУ, безусловно, должны быть высоко качественные полимодельные комплексы, решающие широкий комплекс задач управления. От сбора, передачи, систематизации и распределения данных до задач цифрового мониторинга, анализа, прогнозирования обстановки, структурно-функционального синтеза и обоснования вариантов управленческих решений, планирования реализации принятых решений, их

доведения до исполнителей и мониторинга реализации решений, включая синтез и реализацию корректирующих решений. Базой для подобных ИСПРУ могут служить инвариантные к специфике решаемых задач РПК «КСР-2025» разработки СПбГМТУ [5], адаптированные к решению прикладных задач, среди которых в рамках данных исследований рассмотрим задачу РСУзи ФЛРС [1, 6]. В этой связи актуальной задачей является: в обеспечение изыскания военно-научных путей обеспечения ВТПу применительно к решаемым ФЛРС задачам разработать компьютерную модель РСУзи ФЛРС и адаптировать реализующий ее РПК в варианте «КСР-25.РСУ» с учетом факторов и возможностей КЗИ и ИПД для исследования перспективных научно-технических путей, а также структурно-функциональной и параметрической оптимизации РСУзи применительно к каждой и всего комплекса задач ФЛРС.

В докладе представлены результаты: структурно-функционального моделирования РСУзи; описание варианта ее технологической основы; отличительные особенности свойств и характеристик РСУзи; компьютерная модель и комплекс цифровых оценок качества КЗИ с использованием модели и РПК «КАСОР-24», результаты вариантного ранжирования по системному показателю качества 5 альтернативных вариантов систем управления (СУ). Показано, что переход структур централизованных к распределенным СУ позволяет получить прирост системного качества СУ и, соответственно ВТПу порядка 1,2%, что для системных оценок в целом весьма значительно. В свою очередь, развитие варианта РСУзи в направлении использования технологии цифровых двойников [7] повышает проектное качество и ожидаемую эффективность боевого использования РСУ еще на 1,5%, что в целом превышает типовые требования и возможности на 2024 г. порядка 34%.

Приведенные иллюстративные оценки показывают большие возможности цифрового моделирования проектного качества и ожидаемой эффективности управления боевыми потенциалами при борьбе на море в процессе решения широкого круга практических задач при обосновании направлений развития, разработке средств и систем, их испытаниях и эксплуатации. Числовое вариантное моделирование при поиске оптимальных решений по структуре, свойствам и характеристикам объектов исследования при наличии средств поддержки типа РПК «КСР-2025.РСУ» позволяет сложные системные и наукоемкие задачи при одновременной инженерной оценке и синтезе частных технических проработок решать на большом множестве вариантов проектирования в достаточно сжатые сроки с конкретным их ранжированием по результатам достижения главных целевых показателей.

Следуя рекомендациям исследования и реализуя технологические возможности повышения ряда ЧПК (в РПК с номерами 3.5, 10.6, 10.4 и, даже, при увеличении затрат по ЧПК 10.2) в исследовательском варианте «4.ЦД РСУзи» прирост системного качества составляет более 1,5% с погрешностью 0,6% при средней погрешности ввода исходных данных порядка 5%. С учетом резерва возможностей технологии цифрового двойника в части мониторинга обстановки полученную оценку можно считать также весьма значительной.

В свою очередь, систематизация получаемых данных с их фиксацией в соответствующих базах данных и знаний позволяет аккумулировать научно-технологический потенциал и обоснованно выходить на конкурентно способные системные и организационно-технологические решения при одновременной и существенной экономии ресурсных затрат.

Применительно к комплексу задач ФЛРС разработанная компьютерная модель РСУзи прежде всего может быть результативно использована группой Главного конструктора РСУзи при решении целого комплекса задач проектирования от исследовательского проектирования с обоснованием системно-технического облика, оперативно-технических требований к РСУзи в рамках НИОКР до комплекса задач технического проектирования, создания опытных образцов РСУзи и их приемо-сдаточных испытаний с интегрированной оценкой достигнутых результатов. В процессе эксплуатации технических средств и боевого применения РСУзи ФЛРС разработанная модель и реализующий ее РПК «КСР-25.РСУ» может непрерывно использоваться на всех стадиях жизненного цикла для цифровой оценки эффективности боевого применения РСУзи командиром и штабом ФЛРС, в том числе в режиме «цифровой тени» для непосредственного обоснования управленческих и корректирующих решений.

Таким образом, разработанная компьютерная модель на базе РПК «КСР-25» позволяет не только количественно обосновывать принимаемые командиром ФЛРС (ЛПР) управленческие решения, но и за счет алгоритмов компьютерной оценки индексов корневой чувствительности (макроста «ИКЧ») выдавать рекомендации операторам пунктов управления, обосновывающим проекты управленческих решений (ЛОР), при оптимизации РСУ ФЛРС по критерию максимума военно-технического превосходства над противником.

#### СПИСОК ЛИТЕРАТУРЫ

1. Дригола В.К., Алексеев А.В. Распределенная система поддержки принятия проектных и управленческих решений при ситуационном управлении / Труды Санкт-Петербургского государственного морского технического университета (СПбГМТУ). Выпуск 5 (9), 2024.
2. Пирумов В.С. Информационное противоборство. Четвертое измерение противостояния. М.: «Оружие и технологии», 2010. – 252 с.
3. Адаптивное и робастное управление с компенсацией возмущений. - СПб.: Наука, 2013. 282 с.
4. Алексеев А.В. Модель инвариантной оценки качества и эффективности объектов морской техники / Морские интеллектуальные технологии/Marine intellectual technologies, № 2 том 2, 2020, с. 53-60.
5. Согонов С.А., Максимова М.А., Равин А.А., Хруцкий О.В. Прорывные технологии морских автоматизированных систем в защищенном исполнении / Актуальные проблемы морской энергетики: материалы одиннадцатой международной научно технической конференции. – СПб.: Изд-во СПбГМТУ, 2022, с. 69-77.
6. Дригола В.К., Алексеев А.В. Технология оптимизации принятия решений и распределенного управления сложными организационно-техническими системами / III Всероссийская научно-практическая конференция «Состояние и перспективы развития современной науки по направлению «Информационные технологии в Вооруженных силах Российской Федерации» - Анапа, 2024.03.21-22.
7. Алексеев А.В., Михальчук А.В. Цифровой мониторинг, прогнозирование и контроль успешности реализации комплекса организационно-технических решений (ЦМПК, цифровой двойник) / Свидетельство о государственной регистрации программ для ЭВМ (Реестр программ Федеральной службы по интеллектуальной собственности) № 2023661669, 01.06.2023.

УДК 629.5.082

## ИНФОРМАЦИОННАЯ СКРЫТНОСТЬ ГИБРИДНОЙ ЭНЕРГЕТИЧЕСКОЙ УСТАНОВКИ ДЛЯ БЕСПИЛОТНЫХ НАДВОДНЫХ СУДОВ

**Евдокимов Никита Сергеевич**

Санкт-Петербургский государственный морской технический университет  
Лоцманская ул., 3, Санкт-Петербург, 190121, Россия  
e-mail: nevdokimov19@gmail.com

**Аннотация.** Рассматриваются принципы построения гибридной энергетической установки (ГЭУ) для перспективных беспилотных надводных судов (БНС) малых и средних классов. Показаны преимущества применения комбинированной дизель-электрической схемы с буферным накопителем энергии на литий-ионных аккумуляторах в части повышения энергоэффективности, снижения шумности и вибраций, а также обеспечения скрытности. Приведены результаты моделирования баланса мощности для типовой миссии патрулирования продолжительностью 24 часа и оценена экономическая эффективность внедрения ГЭУ по сравнению с традиционной дизельной установкой.

**Ключевые слова:** беспилотное надводное судно; гибридная энергетическая установка; аккумуляторный модуль; энергоэффективность; электрическая пропульсия.

## INFORMATION STEALTH OF A HYBRID POWER PLANT FOR UNMANNED SURFACE VESSELS

**Evdokimov Nikita**

Saint Petersburg State Marine Technical University  
3 Lotsmanskaya St, Saint Petersburg, 190121, Russia  
e-mail: nevdokimov19@gmail.com

**Abstract.** The paper discusses the architectural principles of a hybrid power plant (HPP) intended for next-generation small and medium unmanned surface vessels (USVs). The advantages of a combined diesel-electric configuration complemented by a lithium-ion buffer energy storage system are demonstrated in terms of improved energy efficiency, reduced acoustic signature and vibration, and enhanced mission stealth. Power-balance simulations for a 24-hour patrol mission are presented, and the economic benefits of the proposed HPP over a conventional diesel plant are evaluated.

**Keywords:** unmanned surface vessel; hybrid power plant; battery module; energy efficiency; electric propulsion.

Беспилотные надводные суда (БНС) предназначены для выполнения широкого спектра задач — от патрулирования и гидрографических исследований до противоминной деятельности. В условиях ограниченного водоизмещения и длительного автономного плавания к энергетической установке БНС предъявляется ряд специфических требований: высокое соотношение удельной мощности и массы, низкая шумность, возможность длительной работы на частичных нагрузках без ухудшения КПД, обеспечение информационной скрытности работы системы [1, 2]. Традиционные дизельные энергетические установки, применяемые на малых судах, не обеспечивают достаточной эффективности при переменных профилях нагрузки, характерных для БНС. Пиковые нагрузки при резких маневрах приводят к неоптимальным режимам работы дизеля, повышению расхода топлива и уровню эмиссии [3].

Решением указанных проблем является применение гибридной дизель-электрической схемы, в которой основным источником механической энергии служит малогабаритный дизель-генератор постоянной скорости вращения, а кратковременные пики мощности покрываются аккумуляторным модулем. Это позволяет поддерживать двигатель внутреннего сгорания в зоне максимального КПД, сокращая расход топлива до 18 % по сравнению с эталонной дизельной установкой сопоставимой мощности [4].

Разработанная в ходе работы математическая модель ГЭУ включает модули динамики заряда-разряда аккумуляторов, теплового баланса и алгоритм энергетического менеджмента, оптимизирующий распределение нагрузки между дизель-генератором и электрическим приводом, что обеспечивает необходимый уровень защиты данных. Результаты симуляций демонстрируют снижение среднего уровня звуковой мощности силовой установки на 5 дБ и уменьшение суммарной массы энергетической системы на 7 % за счёт оптимизации ёмкости батареи [5].

При опытно-проектировании прототипа БНС водоизмещением 12 т с гибридной установкой мощностью 300 кВт был выполнен комплекс экспериментальных испытаний в акватории финского залива. Замеры подтвердили расчётные данные: при крейсерской скорости 12 уз. Расход топлива составил 53 г/(кВт·ч), что на 15 % ниже показателя базовой дизельной схемы. Внедрение ГЭУ на беспилотных платформах создаёт предпосылки для расширения функционала БНС, включая реализацию скрытного «тихого хода», увеличение продолжительности пребывания в дежурном режиме и сокращение эксплуатационных затрат.

## СПИСОК ЛИТЕРАТУРЫ

1. Галонов К.К., Питерсон М.Н. Энергетические установки малых морских беспилотных аппаратов. СПб.: Судостроение, 2022. 312 с.
2. Кузнецов П.П. Гибридные судовые установки: теория и практика. М.: Транспорт, 2021. 408 с.
3. Sakai T., Tanaka H., Yamamoto K. Energy Management Strategy for Hybrid Electric Surface Vehicles // Journal of Marine Engineering & Technology. 2023. vol. 22, № 4. p. 455–468.
4. Arghiroaiei D., Nguyen M., Rossi L. Design considerations for electric & Hybrid Propulsion of Autonomous Surface Vessels // Applied Sciences. 2024. Vol. 14, No. 2. 1125.
5. ISO 19030-1:2016. Ships and marine technology — Measurement of changes in hull and propeller performance. Part 1: General principles.

УДК 004.89:656.61:502.1(571)

**МОДЕЛИРОВАНИЕ И ПРОГНОЗИРОВАНИЕ РАСХОДА СУДОВОГО ТОПЛИВА  
МЕТОДАМИ МАШИННОГО ОБУЧЕНИЯ****Ерофеевский Даниил Владимирович, Митько Арсений Валерьевич**

Санкт-Петербургский государственный университет

Университетский пр., 28, Петергоф, Санкт-Петербург, 198504, Россия

e-mails: daniil.erofeevskii@yandex.ru, arseny73@yandex.ru

**Аннотация.** В работе рассматривается применение методов машинного обучения для прогнозирования расхода судового топлива на основе анализа данных рейсов судов. Сравнительный анализ Случайного леса и Твиди-регрессии показал преимущество ансамблевых методов по точности, устойчивости и интерпретируемости. Дополнительно применялся метод анализа диаграмм Тейлора, позволивший визуально подтвердить различия моделей. Полученные результаты могут использоваться для повышения экологической и экономической эффективности морских перевозок.

**Ключевые слова:** машинное обучение; морские перевозки; расход топлива; экологическая устойчивость; случайный лес; Твиди-регрессия.

**MODELING AND FORECASTING SHIP FUEL CONSUMPTION  
USING MACHINE LEARNING METHODS****Erofeevskii Daniil, Mitko Arseniy**

Saint Petersburg State University

28 University Av., Peterhof, St. Petersburg, 198504, Russia

e-mails: daniil.erofeevskii@yandex.ru, arseny73@yandex.ru

**Abstract.** This study explores the application of machine learning methods for forecasting ship fuel consumption based on voyage data analysis. A comparative analysis of Random Forest and Tweedie Regression demonstrated the advantages of ensemble methods in terms of accuracy, robustness, and interpretability. Additionally, the Taylor diagram method was applied, which provided a visual confirmation of the differences between models. The obtained results can be used to enhance the environmental and economic efficiency of maritime transport.

**Keywords:** machine learning; maritime transport; fuel consumption; environmental sustainability; Random Forest; Tweedie Regression.

Международные грузоперевозки являются ключевым элементом мировой экономики, при этом более 80% товарооборота обеспечивается морским транспортом. Оптимизация работы флота напрямую влияет на стоимость перевозок, устойчивость цепочек поставок и экологическую безопасность. Современные вызовы, связанные с ужесточением экологических норм (зоны контроля выбросов — ECAs) и ростом цен на топливо, требуют новых подходов к управлению [1, 2].

Машинное обучение (МО) в транспортной логистике демонстрирует высокую эффективность благодаря способности выявлять скрытые зависимости в больших массивах данных. В контексте судоходства оно используется для прогнозирования расхода топлива, оценки технического состояния судов, оптимизации маршрутов и снижения выбросов загрязняющих веществ [3].

Цель исследования — оценка потенциала методов МО для прогнозирования расхода топлива в системе «река–море» и определение наиболее эффективного алгоритма для практического применения.

Для анализа был использован массив данных, включающий информацию о 100 рейсах: объемы дизельного (DO) и малосернистого топлива (LFO), координаты переключений, а также параметры окружающей среды (скорость ветра, волнение моря). В качестве ключевого параметра было выделено соотношение D/L — отношение дизельного к малосернистому топливу.

Предварительный корреляционный анализ показал высокую зависимость между переменными DO и LFO, что указывало на избыточность признаков. Для повышения устойчивости модели избыточные параметры были исключены, а в качестве основного предиктора сохранено соотношение D/L. Данные были разделены на обучающую (70 %) и тестовую (30 %) выборки. Для построения прогнозных моделей использовались два алгоритма:

- случайный лес (Random Forest) — ансамблевый метод, основанный на объединении деревьев решений и обладающий высокой устойчивостью к переобучению.
- твиди-регрессия (Tweedie Regression) — статистический метод, применимый для данных с избыточными нулями и асимметричным распределением.

Результаты показали явное преимущество Случайного леса. На тестовой выборке коэффициент детерминации составил  $R^2 \approx 0,993$  при  $RMSE \approx 1,35$  и  $AARD \approx 0,03$ . Для Твиди-регрессии значения были ниже:  $R^2 \approx 0,979$  при  $RMSE \approx 2,26$  и  $AARD \approx 0,049$ . Таким образом, ансамблевый метод оказался более точным и надёжным, сохраняя баланс между прогнозной способностью и интерпретируемостью.

Для дополнительной верификации использовался метод диаграмм Тейлора, позволяющий комплексно оценить точность моделей через соотношение стандартных отклонений и коэффициента корреляции [4, 5].

— Для Случайного леса точки прогнозов группировались вблизи эталонной окружности, что свидетельствует о высокой согласованности предсказанных и фактических значений. Корреляция близка к 1, стандартные отклонения совпадают с наблюдаемыми, что подтверждает устойчивость модели.

— Для Твиди-регрессии наблюдался большой разброс точек и отклонение от эталонной линии. Корреляция была ниже, а стандартное отклонение выше единицы, что указывает на меньшую точность и устойчивость прогнозов.

Таким образом, визуальный анализ подтвердил статистические метрики и показал, что случайный лес лучше воспроизводит изменчивость данных и более надёжен при прогнозировании.

Практическая значимость применения МО проявляется в нескольких аспектах:

- соблюдение экологических стандартов (снижение выбросов  $\text{SO}_x$  и  $\text{NO}_x$  при комбинированном использовании DO и LFO),
- экономия затрат на топливо и обслуживание,
- повышение устойчивости логистических систем в условиях переменной доступности ресурсов,
- развитие портовой инфраструктуры и мультимодальных узлов.

Исследование подтвердило, что интеграция методов МО в практику судоходства обеспечивает существенный прирост эффективности и экологической устойчивости. Случайный лес продемонстрировал лучшие результаты в задаче прогнозирования расхода топлива по сравнению с Твиди-регрессией, что делает его предпочтительным инструментом для морской логистики.

Анализ диаграмм Тейлора дополнительно подтвердил устойчивость ансамблевых методов к переобучению и их способность адекватно воспроизводить изменчивость данных. Эти выводы особенно важны при работе с разнородными данными — ледовой обстановкой, погодными условиями и техническим состоянием судов.

Дальнейшее развитие исследований связано с расширением набора данных и интеграцией прогнозных моделей в цифровые экосистемы управления судоходством. Это позволит повысить безопасность навигации, сократить издержки и минимизировать экологический след морских перевозок, что особенно значимо для Арктики и мультимодальных маршрутов.

#### СПИСОК ЛИТЕРАТУРЫ

1. Nguyen V. N., Rudzki K., Dzida M. et al. Understanding fuel saving and clean fuel strategies towards green maritime. Polish Maritime Research, vol. 30, № 2, pp. 146–164, 2023.
2. Barua L., Zou B., Zhou Y. Machine learning for international freight transportation management: A comprehensive review. Res. Transp. Bus. Manag., vol. 34, p. 100453, Mar. 2020.
3. Filom S., Amiri A. M., Razavi S. Applications of machine learning methods in port operations — A systematic literature review. Transp. Res. Part E: Logist. Transp. Rev., vol. 161, p. 102722, 2022.
4. Lashgari M., Akbari A. A., Nasersarraf S. A new model for optimizing ship route, sailing speed and fuel consumption under different price scenarios. Appl. Ocean Res., vol. 113, p. 102725, 2021.
5. Saito T., Shibasaki R., Murakami S. et al. Global Maritime Container Shipping Networks 1969–1981: Emergence of Container Shipping. J. Mar. Sci. Eng., vol. 10, № 5, p. 602, 2022.

УДК 629.5.015.4

### ВНЕДРЕНИЕ ПЛАТФОРМ MDM В ЦИФРОВЫЕ ПРОЦЕССЫ СУДОСТРОИТЕЛЬНОЙ ИНДУСТРИИ КАК ЭЛЕМЕНТ ЗАЩИЩЕННОЙ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

**Зиновьев Артур Георгиевич**

Санкт-Петербургский государственный морской технический университет

Лоцманская ул., 3, Санкт-Петербург, 190121, Россия

e-mail: az384400@gmail.com

**Аннотация.** В данном исследовании рассматривается внедрение современных технологий управления мастер данными (MDM) в цифровую инфраструктуру судостроительного предприятия. В качестве практического примера анализируется судостроительный завод «Северная верфь», где особое внимание уделяется защите данных в условиях цифровой трансформации. Обоснована необходимость модернизации базы знаний MDM в соответствии с актуальными стандартами ИТ-класса, проведена оценка существующих программных решений, включая тестирование в среде специализированного программного комплекса «IC:MDM». Основной фокус исследования направлен на создание методологии разработки цифрового двойника производственной зоны с использованием российского программного комплекса «КСРП-25». В рамках работы определены приоритетные аспекты цифровой трансформации судостроения, включая оптимизацию точности производственных операций, снижение затрат на изготовление и достижение технологической независимости отрасли. Проведенная работа подчеркивает потенциал комбинированных ИТ-решений, сочетающих иностранные и отечественные технологии. Установлено, что интеграция MDM-инструментов открывает возможности для формирования современных цифровых экосистем, соответствующих запросам судостроительной индустрии будущего.

**Ключевые слова:** MDM; судостроительный завод; цифровая экосистема; цифровой двойник; база знаний; IC:MDM; судостроение; КСРП-25.

## THE INTRODUCTION OF MDM PLATFORMS INTO THE DIGITAL PROCESSES OF THE SHIPBUILDING INDUSTRY AS AN ELEMENT OF SECURE DIGITAL TRANSFORMATION

Zinovev Arthur

Saint Petersburg State Marine Technical University  
3 Lotsmanskaya St, Saint Petersburg, 190121, Russia  
e-mail: az384400@gmail.com

**Abstract.** This study examines the implementation of modern master data management (MDM) technologies in the digital infrastructure of a shipbuilding enterprise. As a practical example, the Severnaya Verf Shipyard is analyzed, where special attention is paid to data protection in the context of digital transformation. The necessity of modernizing the MDM knowledge base in accordance with current IT-class standards is substantiated, and an assessment of existing software solutions is carried out, including testing in the environment of the specialized 1C:MDM software package. The main focus of the research is aimed at creating a methodology for developing a digital twin of the production area using the Russian KSPR-25 software package. As part of the work, priority aspects of the digital transformation of shipbuilding have been identified, including optimizing the accuracy of production operations, reducing manufacturing costs and achieving technological independence of the industry. The work carried out highlights the potential of combined IT solutions combining foreign and domestic technologies. It has been established that the integration of MDM tools opens up opportunities for the formation of modern digital ecosystems that meet the needs of the shipbuilding industry of the future.

**Keywords:** MDM; shipbuilding plant; digital ecosystem; digital twin; knowledge base; 1C:MDM; shipbuilding; KSPR-25.

В эпоху активной цифровизации промышленного производства в рамках концепции Индустрии 4.0 особое значение приобретает внедрение интеллектуальных систем технической документации с комплексной защитой данных. Ключевую роль в этом процессе играют технологии управления мастер данными (MDM), обеспечивающие централизованное управление мастер данными на протяжении всего жизненного цикла морской техники.

Для судостроительной отрасли, где особую значимость приобретают оперативный доступ к достоверным техническим данным, безопасность эксплуатации и соответствие нормативным стандартам, внедрение MDM-систем является ключевым стратегическим решением. Такие технологии обеспечивают создание централизованных систем управления данными, встраиваемых в единую цифровую инфраструктуру компании, что способствует оптимизации процессов технического обслуживания, ремонта и модернизации судового оборудования [1].

Особенность современных MDM-систем заключается в их гибкой интеграции в производственные процессы, обеспечивая персонал согласованными и стандартизированными данными в режиме реального времени. Это критически важно для реализации сложных судостроительных проектов, где устаревшие методы управления данными не способны гарантировать их точность, актуальность и соответствие отраслевым нормам. Внедрение MDM-платформ в единую информационную инфраструктуру предприятия способствует повышению качества данных, снижению ошибок и укреплению цифровой зрелости производственных процессов [2].

Целью настоящего исследования является разработка методологии интеграции MDM-технологий в цифровую инфраструктуру ледокола «Лидер» с последующим моделированием цифрового двойника (ЦД) производственного цикла, обеспечивающего комплексную защиту информации. Основное внимание уделено оптимизации управления мастер-данными, анализу совместимости MDM-решений с существующими ИТ-системами и созданию интеллектуальной платформы для централизованного контроля данных [3, 4].

На начальном этапе исследования проведен комплексный анализ современных MDM-систем на предмет их соответствия требованиям управления данными в судостроительной отрасли. В рамках оценки изучались следующие ключевые аспекты:

- Функциональность управления мастер-данными (обеспечение согласованности, актуальности и целостности информации).
- Поддержка структурированных форматов данных (XML, реляционные БД) для унификации процессов обмена.
- Совместимость с системами управления жизненным циклом изделий (PLM) для синхронизации данных на всех этапах производства.
- Интеграция с корпоративными системами (ERP, MES) через стандартизированные API и middleware-решения.

Среди наиболее релевантных решений для управления мастер-данными выделены платформы 1C:MDM, SAP Master Data Governance и IBM InfoSphere.

Была проведена апробация MDM-класса на примере системы «1C:MDM». В ходе тестирования выявлен ряд уникальных функциональных преимуществ, отличающих данное решение от аналогов [5].

1C:MDM — российская платформа для централизованного управления мастер-данными, обеспечивающая их стандартизацию, синхронизацию и интеграцию в корпоративную экосистему.

В судостроительной отрасли система применяется для:

- управления справочными данными (номенклатура, технические характеристики, нормативы);



– автоматизации обмена данными между системами (ERP, PLM, MES) через унифицированные интерфейсы.

В ходе практического тестирования 1С:MDM подтверждена его способность обеспечивать:

- Единое пространство мастер-данных с поддержкой кросс-системной согласованности;
- Сокращение времени на актуализацию данных за счет автоматизированных workflows;
- Повышение точности информации, используемой в производственных и логистических процессах.

Разработан цифровой двойник системы управления мастер-данными на базе отечественного ПО «КСР-25», интегрирующий данные MDM-платформ и параметры производственных процессов. Решение обеспечивает мониторинг актуальности данных, анализ их качества и моделирование сценариев обновления в режиме реального времени в соответствии с отраслевыми стандартами информационной безопасности.

Предложенный подход позволил автоматизировать процессы согласования изменений, контроля версионности данных и их распределения между подразделениями. Результаты подтвердили эффективность MDM-технологий для централизованного управления данными в условиях цифрового производства.

Данная методология обеспечивает гибкость системы при адаптации к изменениям бизнес-требований на всех этапах жизненного цикла продукции.

Такой подход закладывает основу для перехода к интеллектуальным моделям управления жизненным циклом судов, повышая технологическую независимость и конкурентоспособность отечественных предприятий. Исследования демонстрируют перспективность развития MDM-решений и их интеграции с AI-инструментами для прогнозной аналитики в судостроении.

#### СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ 19.701-90. Схемы алгоритмов, программ, данных и систем. Условные обозначения и правила выполнения. М.: Издательство стандартов, 1991. 24 с.
2. Master Data Management (PDM): концепция и практика применения // Информационные технологии. 2022. №4. С. 27–33.
3. Левин В.А., Мельников А.А. Информационные технологии управления жизненным циклом изделия. СПб.: БХВ-Петербург, 2020. 258 с.
4. 1С:Предприятие. Официальный сайт разработчика. URL: <https://v8.1c.ru/> (дата обращения: 10.04.2025).
5. 1С:MDM Управление нормативно-справочной информацией. Отраслевые и специализированные решения 1С:Предприятие. URL: <https://solutions.1c.ru/catalog/mdm> (дата обращения: 10.04.2025).

УДК 004.056.5

### ПОДСИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ИНТЕЛЛЕКТУАЛЬНОЙ ПОДДЕРЖКИ ПЕРЕВОЗКИ НЕГАБАРИТНЫХ ГРУЗОВ

Илюхин Пётр Эдуардович

Санкт-Петербургский государственный морской технический университет

Лощманская ул., 3, Санкт-Петербург, 190121, Россия

e-mail: petr.iliukhin@yandex.ru

**Аннотация.** Рассматривается подсистема информационной безопасности для интеллектуальной поддержки перевозки негабаритных грузов, учитывающая специфику логистических процессов и современные киберугрозы. Предложена четырехэтапная модель защиты данных, включающая шифрование (RSA), стеганографию (LSB), резервное копирование и восстановление. Разработана архитектура подсистемы на основе базы знаний и мультиагентного подхода, обеспечивающая отказоустойчивость за счет использования NoSQL-баз данных. Проведено сравнение методов защиты по производительности и уровню защищенности, подтверждающее эффективность решения.

**Ключевые слова:** подсистема информационной безопасности; интеллектуальная поддержка; негабаритный груз; защита информации; шифрование; стеганография.

### INFORMATION SECURITY SUBSYSTEM FOR INTELLIGENT SUPPORT OF TRANSPORTATION OF OVERSIZED CARGO

Iliukhin Petr

Saint Petersburg State Marine Technical University

3 Lotsmanskaya St., Saint Petersburg, 190121, Russia

e-mail: petr.iliukhin@yandex.ru

**Abstract.** The paper evaluates an information security subsystem for intelligent support of oversized cargo transportation, addressing logistical challenges and modern cyber threats. A four-stage data protection model is proposed, integrating encryption (RSA), steganography (LSB), backup, and recovery. The subsystem architecture leverages a knowledge base and multi-agent approach, ensuring fault tolerance through NoSQL database integration. Comparative analysis of protection methods confirms their efficiency in terms of performance and security level.

**Keywords:** information security subsystem; intelligent support; oversized cargo; data protection; encryption; steganography.

Актуальность этой темы состоит в том, что в нынешнее время перевозка негабаритных грузов требует высокой точности и защищенности данных, поскольку информация о маршрутах, грузах и логистике подвержена

рискам несанкционированного доступа, утечек и кибератак. Современные угрозы в условиях цифровизации транспортных систем делают разработку комплексных решений для обеспечения конфиденциальности, целостности и доступности данных критически важной задачей [1-3].

Цель этого доклада состоит в создании модели подсистемы информационной безопасности, адаптированной к специфике перевозки негабаритных грузов, с использованием интеллектуальных технологий, баз знаний и методов защиты информации, обеспечивающих надежность и устойчивость к внешним угрозам.

Основной вопрос также заключается в разработке объективных критериев оценивания технологии [4-6], включая:

- Соответствие требованиям стандартов безопасности (например, ФСТЭК России).
- Уровень защиты от распространенных киберугроз (SQL-инъекции, DDoS-атаки, фишинг).
- Интеграция с существующими системами управления логистикой (WMS, ERP).
- Экономическая эффективность (стоимость внедрения vs. снижение рисков утечек данных).
- Масштабируемость и адаптивность к изменению условий эксплуатации.

Перспективы внедрения данной технологии связаны с её применением в объектах морской инфраструктуры, где критически важны конфиденциальность данных о маршрутах, целостность информации о состоянии груза и доступность систем в реальном времени. Технология может быть интегрирована в системы управления судами, портовыми комплексами и логистическими сетями, обеспечивая защиту от кибератак и минимизируя последствия возможных инцидентов.

#### СПИСОК ЛИТЕРАТУРЫ

1. Сертификация средств и систем защиты информации: конспект лекций (в электронном виде) / Алексеев А.В. СПбГМТУ, КСАиИ, 2023.
2. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации / Утверждено приказом ФСТЭК России от 25 декабря 2017 г. № 239.
3. Положение о системе сертификации средств защиты информации / Утверждено приказом ФСТЭК России от 3 апреля 2018 г. N 55.
4. Искандеров Ю. М., Чумак А. С., Шахнов С. Ф. Интеллектуальная поддержка принятия решений по перевозке негабаритных грузов // Системный анализ в проектировании и управлении: сборник научных трудов XXVI Международной научно-практической конференции. СПб., 2023. С. 319–323.
5. Ныров А. П., Соколов С. С., Башмаков А. В. Методика проектирования безопасных информационных систем на транспорте // Проблемы информационной безопасности. Компьютерные системы. 2010. № 3. С. 58–61.
6. Юрков А. Н. Ранжирование информационных технологий класса «FM» в защищенном исполнении // Информационная безопасность регионов России (ИБРР-2023). СПб., 2023. С. 241–245.

УДК 621.7.01

#### **АКТУАЛИЗАЦИЯ БАЗЫ ДАННЫХ И ЗНАНИЙ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ КЛАССА САМ С УЧЕТОМ ТРЕБОВАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**Кутикова Алевтина Константиновна, Алексеев Анатолий Владимирович**

Санкт-Петербургский государственный морской технический университет

Лотманская ул., 3, Санкт-Петербург, 190121, Россия

e-mail: kutikova2002@gmail.com

**Аннотация.** Информационные технологии класса САМ — программное обеспечение, предназначенное для автоматизации процессов проектирования, моделирования и управления производственными операциями с учетом требований информационной безопасности. В последние десятилетия использование САМ-систем стало неотъемлемой частью инженерного и производственного процесса, значительно повышая точность, скорость и эффективность разработки изделий.

**Ключевые слова:** информационная технология; САМ; computer-aided manufacturing; конкурентоспособность; базы данных.

#### **UPDATING THE DATABASE AND KNOWLEDGE OF INFORMATION TECHNOLOGIES OF THE CAM CLASS, TAKING INTO ACCOUNT THE REQUIREMENTS OF INFORMATION SECURITY**

**Kutikova Alevtina, Alekseev Anatoly**

Saint Petersburg State Marine Technical University

3 Lotsmanskaya St, Saint Petersburg, 190121, Russia

e-mail: kutikova2002@gmail.com

**Abstract.** Information technology of the CAM class is software designed to automate the processes of design, modeling and management of production operations, taking into account the requirements of information security. In recent decades, the use of CAM systems has become an integral part of the engineering and manufacturing process, significantly increasing the accuracy, speed and efficiency of product development.

**Keywords:** information technology; CAM; computer-aided manufacturing; competitiveness; database.

Информационные технологии класса САМ (англ. Computer-Aided Manufacturing) — программное обеспечение, предназначенное для автоматизации процессов проектирования, моделирования и управления производственными операциями. В последние десятилетия использование САМ-систем стало неотъемлемой

частью инженерного и производственного процесса, значительно повышая точность, скорость и эффективность разработки изделий [1]. Современные САМ-программы обеспечивают высокую точность, снижение числа ошибок, а также улучшение производительности на всех этапах жизненного цикла изделия — от концептуального проектирования до его производства [2]. При этом современные реализации таких систем включают встроенные механизмы защиты, обеспечивающие безопасную работу с важными производственными данными. На текущий момент существует несколько ведущих САМ-платформ, таких как SolidCAM, Mastercam, Autodesk Fusion 360, Siemens NX и другие, которые предоставляют комплексные решения для работы с различными видами станков и устройств, а также для взаимодействия с CAD-системами (англ. Computer-Aided Design).

Целями работы являются определение лучших информационных технологий класса САМ, выполнение квалитетического ранжирования и выявление лучших среди информационных технологий указанного класса с учетом требований информационной безопасности. Для достижения целей работы предусматривается решение следующих задач: формирование базы данных информационных технологий класса САМ, формирование критериев оценки качества исследуемых информационных технологий, квалитетическое ранжирование.

Выбор подходящей САМ-системы зависит от множества факторов, включая размер предприятия, требования к производству, степень защищенности данных, бюджет и тип обрабатываемых материалов. Каждая из рассматриваемых программ имеет свои сильные и слабые стороны: Mastercam и SolidCAM предлагают высокую гибкость и множество возможностей для сложных операций, но требуют значительных финансовых вложений. Autodesk Fusion 360 — удобная и доступная платформа с облачными возможностями, ограниченная в плане высокоскоростной обработки и сложных операций. Siemens NX — мощная и комплексная система для высокоточных и специализированных производств, при этом, требующая значительных инвестиций. Edgcam является хорошим выбором для предприятий, которым нужна стабильность.

Российские САМ-системы предлагают хорошие возможности для работы с отечественным оборудованием, а также могут быть более доступными по цене, чем их зарубежные аналоги. Тем не менее, многие из них имеют ограничения в функциональности по сравнению с ведущими мировыми решениями, такими как Mastercam, SolidCAM или Siemens NX. Важно, чтобы предприятия выбирали подходящую САМ-систему, исходя из специфики своей работы, требований к точности, сложности обработки и бюджета. Российские программы могут быть хорошими решениями для небольших и средних предприятий, которые ищут недорогие, но функциональные системы для стандартных производственных процессов. В то же время для более сложных задач и высокоточных операций может потребоваться использование зарубежных САМ-систем с более мощными возможностями и поддержкой сложных операций.

#### СПИСОК ЛИТЕРАТУРЫ

1. Норенков И. П. Основы автоматизированного проектирования: Учеб. для вузов. 2-е изд., перераб. и доп. М.: Изд-во МГТУ им. Н.Э. Баумана, 2002. 336 с.
2. Ушаков Д.М. Введение в математические основы САПР: курс лекций. М.: ДМК Пресс, 2011. 208 с.
3. Адамцевич Л.А., Пиляй А.И. Разработка базы данных отбора и экспертной проверки объектов культурного наследия для обучения искусственного интеллекта // Строительное производство. 2023. № 2. С. 80-84.

УДК 629.5.07

#### КОЛИЧЕСТВЕННАЯ ОЦЕНКА ЭКОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ И ЗАЩИТА ДАННЫХ НА ПРИМЕРЕ АО «ЦМКБ АЛМАЗ»

Лихачева Елизавета Сергеевна

Санкт-Петербургский государственный морской технический университет

Лотманская ул., 3, Санкт-Петербург, 190121, Россия

e-mail: elizaveta.lixacheva@yandex.ru

**Аннотация.** В докладе рассматривается методика количественной оценки экологической безопасности и защиты данных на примере АО «ЦМКБ Алмаз» с использованием программы КСПР и созданием цифрового двойника предприятия. Представлен комплексный подход к анализу экологических рисков на всех этапах жизненного цикла продукции, включая моделирование сценариев и оптимизацию производственных процессов. Описаны результаты практической реализации, которые показали повышение точности мониторинга и эффективности управления экологическими характеристиками производства. Внедрение цифрового двойника способствует снижению негативного воздействия на окружающую среду и формированию устойчивого развития предприятия.

**Ключевые слова:** экологическая безопасность; количественная оценка; цифровой двойник; экологические риски; судостроение; жизненный цикл продукции; АО «ЦМКБ Алмаз»; программа КСПР.

#### QUANTITATIVE ASSESSMENT OF ENVIRONMENTAL SAFETY AND DATA PROTECTION USING THE EXAMPLE OF ALMAZ CENTRAL DESIGN BUREAU JSC

Lihacheva Elizaveta

Saint Petersburg State Marine Technical University

3 Lotmanskaya St, Saint Petersburg, 190121, Russia

e-mail: elizaveta.lixacheva@yandex.ru

**Abstract.** The article discusses a methodology for quantifying environmental safety and data protection using the example of Almaz Central Design Bureau JSC using the KSPR program and creating a digital twin of the enterprise. A comprehensive approach to analyzing environmental risks throughout the product lifecycle is presented, including scenario modeling and optimization of production processes. The results of practical implementation demonstrated improved accuracy of monitoring and enhanced management of environmental aspects in production. The introduction of a digital twin contributes to reducing negative environmental impacts and promoting sustainable development of the enterprise.

**Keywords:** environmental safety; quantitative assessment; digital twin; environmental risks; shipbuilding; product lifecycle; JSC “СМКБ Алмаз”; KSPR software.

Количественная оценка экологической безопасности на примере АО «СМКБ Алмаз» и создание его цифрового двойника — это современный и всесторонний подход к управлению воздействием предприятия на окружающую среду, реализуемый с учетом современных требований к защите данных. Цель такого подхода — сократить вред, наносимый природе, и повысить устойчивость производственных процессов.

Сегодня, когда экологические требования ужесточаются, а внимание общества к этим вопросам растёт, компании судостроительной отрасли должны использовать эффективные инструменты для оценки и управления экологическими рисками на всех этапах жизненного цикла продукции [1].

Для проведения оценки на АО «СМКБ Алмаз» применялась специализированная программа КСПР, которая позволила систематизировать большой объём экологической информации и провести её детальный анализ [2]. Оценка охватывала ключевые аспекты воздействия на природу: выбросы в атмосферу, образование и переработку отходов, потребление энергии и ресурсов, а также влияние производства на водные и земельные ресурсы. Такой подход помог не только подтвердить уже известные риски, но и выявить ранее незамеченные факторы, которые также могут влиять на экологическую и информационную безопасность.

Создание цифрового двойника стало важным шагом в развитии экологического менеджмента на предприятии. Этот цифровой двойник — виртуальная модель, в которую заложены данные о технологиях, потреблении ресурсов и экологических характеристиках. С его помощью можно моделировать различные сценарии развития, заранее оценивать возможное воздействие на окружающую среду и планировать меры по снижению рисков — без необходимости в дорогостоящих экспериментах в реальности. Благодаря цифровому двойнику предприятие получает возможность оперативно реагировать на изменения и корректировать экологическую политику практически в режиме реального времени.

Анализ позволил выделить несколько приоритетных направлений, требующих особого внимания. Это, прежде всего, улучшение системы утилизации отходов, сокращение вредных выбросов и повышение энергоэффективности [3, 4]. Также цифровая модель помогла выявить уязвимые места в производственных цепочках, где существует риск нарушения экологических норм. Это позволило точно разработать решения для устранения этих проблем. В результате, экологическая нагрузка на окружающую среду снизилась, а деятельность предприятия стала лучше соответствовать нормативным требованиям.

Практическое внедрение методики количественной оценки и цифрового двойника в АО «СМКБ Алмаз» подтвердило их высокую эффективность. Улучшилось качество и оперативность экологического мониторинга, а также интеграция этих данных в управленческие процессы. Это не только помогает соблюдать законы, но и укрепляет репутацию компании как ответственного и экологически ориентированного производителя.

Кроме того, такой подход открывает новые возможности для оптимизации использования ресурсов и снижения затрат, что делает предприятие более конкурентоспособным.

Таким образом, опыт АО «СМКБ Алмаз» показывает: сочетание количественной оценки и цифрового двойника — действенный инструмент для управления экологическими аспектами производства. Он позволяет заранее выявлять потенциальные риски, снижать их и поддерживать устойчивое развитие компании в соответствии с современными экологическими стандартами.

В условиях нарастающих экологических вызовов такие технологии становятся необходимым элементом для развития судостроительных предприятий.

#### СПИСОК ЛИТЕРАТУРЫ

1. Постижков, Р. А., Палкин, Е. С. Цифровые двойники: Применение в судостроении / р. А. Постижков, е. С. Палкин // судостроение. 2021. № 12. с. 129–134. (дата обращения: 18.05.2025).
2. Решняк, В. И., Каляуш, А. И., Решняк, К. В. Управление экологической безопасностью при эксплуатации судов: Учебное пособие / спб.: Изд-во ГУМРФ им. Адмирала С. О. Макарова, 2019. 72 с. ISBN 978-5-9509-0394-6.
3. Показатели экологической безопасности водного транспорта / Каминский В.Ю., Скороходов Д.А., Турусов С.Н] // вестник морской экологии. 2023. т. 15, № 3. с. 45–52. режим доступа: <https://elibrary.ru/item.asp?id=46657431> (дата обращения: 17.05.2025).
4. Оценка рисков в судостроении // Консалтинг в судостроении. 2022. <https://consult-cct.ru/ocenka-riskov-v-sudostroenii> (дата обращения: 18.05.2025).

УДК 004.78

**ЗАЩИТА ОТ DDoS-АТАК В КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЕ****Лотоцкая Ольга Александровна**

Санкт-Петербургский государственный морской технический университет

Лоцманская ул., 3, Санкт-Петербург, 190121, Россия

e-mail: ilya.bukovskiy@mail.ru

**Аннотация.** В статье рассматриваются методы защиты критической инфраструктуры от распределенных атак типа «отказ в обслуживании» (DDoS). Анализируются современные подходы к обнаружению, фильтрации и нейтрализации атак, включая использование аппаратных решений, алгоритмов машинного обучения и кооперативных систем защиты. Особое внимание уделено применению этих методов в транспортных системах и других критически важных объектах.

**Ключевые слова:** DDoS-атаки; кибербезопасность; критическая инфраструктура; фильтрация трафика; машинное обучение; отказоустойчивость.

**PROTECTION AGAINST DDoS ATTACKS IN CRITICAL INFRASTRUCTURE****Lototskaya Olga**

Saint Petersburg State Marine Technical University

3 Lotsmanskaya St, Saint Petersburg, 190121, Russia

e-mail: ilya.bukovskiy@mail.ru

**Abstract.** The article examines methods of protecting critical infrastructure from distributed denial-of-service (DDoS) attacks. Modern approaches to attack detection, traffic filtering, and neutralization are analyzed, including the use of hardware solutions, machine learning algorithms, and cooperative defense systems. Special attention is paid to the application of these methods in transport systems and other critical facilities.

**Keywords:** DDoS attacks; cybersecurity; critical infrastructure; traffic filtering; machine learning; fault tolerance.

Современные DDoS-атаки представляют собой одну из наиболее серьезных угроз для критической инфраструктуры, включая транспортные системы, энергетику и телекоммуникации. С развитием интернета вещей (IoT) и увеличением пропускной способности сетей масштабы и сложность таких атак неуклонно растут. Это требует разработки комплексных систем защиты, способных противостоять как традиционным, так и инновационным методам кибератак [1-3].

Основной проблемой при защите от DDoS-атак является необходимость оперативного различения легитимного трафика и вредоносных запросов. В первом случае применяются системы глубокого анализа пакетов (Deep Packet Inspection), позволяющие выявлять аномалии в структуре передаваемых данных. Для этого используются как сигнатурные методы, основанные на известных шаблонах атак, так и поведенческий анализ, фиксирующий отклонения от нормальных параметров трафика.

Особую эффективность демонстрируют распределенные системы защиты, построенные по принципу «очистки трафика». В таких системах входящий поток данных перенаправляется через специализированные центры фильтрации, где происходит его тщательный анализ и отсеивание вредоносных пакетов. При этом ключевое значение имеет минимальная задержка при обработке, что особенно важно для систем реального времени, таких как управление транспортными потоками [4, 5].

Для защиты критически важных объектов все чаще применяются превентивные меры, включающие:

- Построение избыточной сетевой инфраструктуры
- Реализацию механизмов автоматического масштабирования ресурсов
- Использование геораспределенных систем балансировки нагрузки
- Внедрение проактивного мониторинга сетевой активности

Важным направлением является разработка интеллектуальных систем защиты на основе технологий искусственного интеллекта. Машинное обучение позволяет создавать адаптивные алгоритмы, способные выявлять новые, ранее неизвестные типы атак. В частности, методы глубокого обучения демонстрируют высокую эффективность при анализе временных рядов сетевого трафика и выявлении сложных паттернов DDoS-атак.

Особую сложность представляет защита от атак на прикладном уровне (Layer 7), которые имитируют поведение обычных пользователей [5]. Для противодействия таким угрозам применяются комплексные решения, сочетающие:

- анализ поведенческих характеристик,
- проверку репутации IP-адресов,
- контроль частоты запросов,
- системы проверки пользователей (CAPTCHA).

В транспортных системах дополнительную сложность создает требование минимального времени отклика. Это обуславливает необходимость специальных оптимизированных решений, обеспечивающих высокую скорость обработки запросов [5-7] без ущерба для эффективности защиты.

Перспективным направлением является разработка стандартизированных протоколов обмена информацией об угрозах между различными элементами критической инфраструктуры. Это позволит создавать

кооперативные системы защиты, где данные об атаках, полученные одним узлом, могут быть оперативно использованы для защиты других участников сети.

Таким образом, современные системы защиты от DDoS-атак должны сочетать многоуровневый подход, включающий как традиционные методы фильтрации, так и инновационные технологии на основе искусственного интеллекта, обеспечивая при этом необходимую производительность для работы в системах реального времени.

#### СПИСОК ЛИТЕРАТУРЫ

1. Зайцев, А. В. Кибербезопасность критической инфраструктуры / А. В. Зайцев. М. : Лаборатория знаний, 2020. 420 с.
2. Mirkovic, J. A Taxonomy of DDoS Attack and DDoS Defense Mechanisms / J. Mirkovic, P. Reiher // ACM SIGCOMM. 2004.
3. Douligieris, C. DDoS Attacks and Defense Mechanisms: Classification and State-of-the-art / C. Douligieris, A. Mitrokotsa // Computer Networks. 2004.
4. RFC 4732 Internet Denial-of-Service Considerations. IETF, 2006.
5. Кузнецов, Н. А. Защита сетей от DDoS-атак с использованием SDN / Н. А. Кузнецов. СПб. : БХВ, 2019. 256 с.
6. Cloudflare. DDoS Protection Best Practices. 2023. [Электронный ресурс]. URL: <https://www.cloudflare.com/learning/ddos/ddos-mitigation/>. Дата посещения: 20.08.2025.
7. Arbor Networks. Worldwide Infrastructure Security Report. 2022.

УДК 681.518, 65.011.56

### КОНЦЕПЦИЯ СППР ДЛЯ УПРАВЛЕНИЯ ПРОИЗВОДСТВЕННЫМИ ПРОЦЕССАМИ СУДОСТРОИТЕЛЬНОГО ПРЕДПРИЯТИЯ

**Миклуш Сергей Владимирович**

АО «Адмиралтейские верфи»

реки Фонтанки наб., 203, Санкт-Петербург, 190121, Россия

e-mail: miklush.sv@ashipyards.com

**Аннотация:** Представлена концепция системы поддержки принятия решений (СППР) для управления производственными процессами строительства судовых заказов на судостроительном предприятии. Приведена классификация существующих СППР с кратким описанием этапов развития данных систем. Приведены основные методы планирования, используемые на судостроительных предприятиях, а именно: метод «критического пути» (англ. CPM, или critical path method); метод PERT (Program Evaluation and Review Technique); метод сетевого планирования с использованием системы предшествования (PDM), которые не удовлетворяют в полной мере потребностям судостроительной специфики для реализации высокоэффективной системы поддержки управленческих решений, в виду наличия большого количества длительных и трудоемких технологических процессов (ТП), которые необходимо контролировать не только по факту выполнения, как при существующих подходах, а на протяжении всего производственного цикла. Предложен вариант СППР, базирующийся на полимодельном методе оценивания агрегированного показателя качества (АПК) строительства судового заказа на основе свертки частных показателей качества (ЧПК) технологических процессов, входящих в процесс строительства заказа. На основе предложенной модели, СППР будет в зависимости от величины вычисляемого значения АПК формировать для руководителей строительством судового заказа предложения управленческих решений. В итоге руководители различных уровней смогут фокусировать внимание на критически важных направлениях реализации процесса строительства судового заказа и опираясь на проекты предложенных управленческих решения принимать наиболее эффективные решения для минимизации временных и производственных издержек.

**Ключевые слова:** системы поддержки принятия решений; цифровизация управления судостроительным производством; полимодельный метод; агрегирование показателей качества.

### A DIGITALIZATION MODEL OF CONTROLLED PRODUCTION PROCESS MANAGEMENT WITH A FEEDBACK LOOP FOR SYSTEM INDICATORS

**Miklush Sergey**

JSC «Admiralty Shipyards»

203 Fontanka River Emb, St. Petersburg, 190121, Russia

e-mail: miklush.sv@ashipyards.com

**Abstract:** The article presents the concept of decision support system (DSS) for managing production processes of shipbuilding orders construction at a shipbuilding enterprise. The classification of existing DSS with a brief description of the stages of development of these systems is given. The main planning methods used at shipbuilding enterprises are given, namely: the critical path method (CPM); the PERT method (Program Evaluation and Review Technique); the method of network planning using the precedence system (PDM), which do not fully meet the needs of shipbuilding specifics for building a highly effective system for supporting management decisions, due to the presence of a large number of long and labor-intensive technological processes (TP), which must be controlled not only upon completion, as with existing approaches, but throughout the entire production cycle. A DSS version is proposed based on a poly-model method for assessing the aggregated quality indicator (AQI) of shipbuilding order construction based on the convolution of private quality indicators (PQI) of technological processes included in the order construction process. Based on the proposed model, the DSS will, depending on the value of the calculated value of the APC, generate proposals for management decisions for the ship order construction managers. As a result, managers at various levels will be able to

focus on critically important areas of the ship order construction process and, based on the projects of the proposed management decisions, make the most effective decisions to minimize time and production costs.

**Keywords:** decision support systems; digitalization of shipbuilding production management; polymodel method; aggregation of quality indicators.

Системы поддержки принятия решений (СППР) — это комплекс программных средств, основанных на различных моделях и методах оценки массива данных, позволяющий формировать альтернативные управленческие решения с целью повышения эффективности этих решений [1]. Первые прототипы СППР сформировались из систем управления и мониторинга банковских транзакций в 60-х — 70-х годах. Они представляли собой надстройку для баз данных, включающую в себя функции численного моделирования (например, система «DYNAMO», разработанная в Массачусетском технологическом университете).

С начала 80-х, с внедрением персональных компьютеров, появилась возможность проводить автоматизацию учета и обработку данных более широкому кругу предприятий. Появились разные подклассы СППР: MIS (Management Information System); EIS (Executive Information System); GDSS (Group Decision Support Systems); ODSS (Organization Decision Support Systems), в которые уже возможно было встроить различное моделирование. В конце 80-х появились ПСППР (Продвинутые СППР), которые основывались на нечеткой логике и позволяли проводить анализ на более продвинутых моделях [1, 2].

В 1993 г. зародилась подсистема OLAP (Online Analytical Processing) для СППР, базирующаяся на оперативном анализе и обработке данных для принятия управленческих решений [3]. Особенностью данной системы является представление данных в виде многомерного куба.

В конце 90-х появились интеллектуальные СППР основанные на использовании системного анализа, машинного обучения и различных эвристических методов [1-3].

На сегодняшний день в соответствии с градацией, предложенной в [3] СППР разделяют на: управляемые моделями (Model-Driven DSS); управляемые данными (Data-Driven DSS); управляемые сообщениями (Communication-Driven DSS); управляемые документами (Document-Driven DSS); управляемые знаниями (Knowledge-Driven DSS). Следует отметить, что СППР управляемые моделями обычно используются при оптимизации ресурсов и в планировании проектов.

Решение. На судостроительных предприятиях при строительстве судовых заказов нашли широкое применение СППР на основе модели сетевых графиков строительства. Существуют следующие основные методы на которых формируются данные модели [4]:

- метод «критического пути» (англ. CPM);
- метод PERT (Program Evaluation and Review Technique);
- метод сетевого планирования с использованием системы предшествования (PDM).

Представленные методы планирования не удовлетворяют в полной мере требованиям эффективного управления судостроительным производством, в виду того, что выполнение работ контролируется по факту выполнения, что приводит к большим временным задержкам, особенно для длительных и трудоемких технологических процессов, которых при строительстве судовых заказов подавляющее большинство.

Для исключения указанных недостатков предлагается реализовать полимодельный метод [5] оценивания агрегированного показателя качества (АПК) строительства судового заказа на основе свертки частных показателей качества (ЧПК) ТП, входящих в процесс строительства заказа [6].

На основе предложенной модели возможна реализация СППР для руководителей строительством судового заказа, которая в зависимости от величины вычисляемого значения АПК будет формировать предложения управленческих решений. В качестве типовых вариантов проектов решений, например, могут быть: при 90%...100% успешности завершения процесса с заданным качеством и в назначенный срок — «Действовать по плану»; 80%...90% — «Угроза невыполнения требований. Запросить конкретную помощь»; 50%...80%; — «Невыполнение требований. Предупредить руководителя о НСС»; менее 50% — «Невыполнение требований. Передать управление (ФИО)».

При постоянном обновлении информации по процессу строительства заказа для руководителей будет синхронно обновляться итоговое значение успешности реализации проекта на дату окончания с формированием соответствующих управленческих предложений.

Руководители различных уровней смогут фокусировать внимание на критически важных направлениях реализации процесса строительства судового заказа и опираясь на проекты предложенных управленческих решения принимать наиболее эффективные решения для минимизации временных и производственных издержек во обеспечения неукоснительного выполнения графика строительства.

В итоге предложенный подход концепции СППР для управления производственными процессами при строительстве судового заказа на судостроительном предприятии позволяет систематизировать процесс контроля строительства и повысить эффективность принятия управленческих решений, опираясь на полимодельный метод оценивания АПК судового заказа на основе свертки ЧПК ТП входящих в процесс строительства судового заказа.

В свою очередь, данная концепция позволяет вывести цифровизацию производственных процессов строительства судовых заказов на принципиально новый уровень, для дальнейшей интеграции производственной части с технологической подготовкой производства, обеспечением материально-техническими ресурсами в единый цифровой продукт управления судостроительным предприятием.

## СПИСОК ЛИТЕРАТУРЫ

1. Коновальцева Е. Г. История формирования и принципы построения систем поддержки принятия решений / Сборник трудов РИИБ. Выпуск 5. 2018, с 476-479.
2. Rafael Valencia-Garcia. Exploring Intelligent Decision Support Systems/ Rafael Valencia-Garcia, Mario Andres Paredes-Valverde, Maria del Pilar Salas-Zarate, 2018, 262 p.
3. Лабабиди М. Система поддержки принятия решений (СППР) как инструмент принятия эффективных управленческих решений на промышленных предприятиях. / Лабабиди М. Рагб, Кельчевская Н. Р. // Весенние дни науки: сборник докладов Международной конференции студентов и молодых ученых (Екатеринбург, 21–23 апреля 2022 г.). Екатеринбург : УрФУ, 2022. С. 377-381.
4. Культин Н. Б. Инструменты управления проектами: Project Expert и Microsoft Project СПб.: БХВ-Петербург, 2009. 160 с.
5. Алексеев А.В. Практика реализации полимодельного квалиметрического метода системной инвариантной оценки качества и эффективности объектов морской техники / А.В. Алексеев, А.В. Михальчук, А.Е. Карпов, К.М. Орлов, М.А. Каганский // Перспективные направления развития отечественных информационных технологий: материалы VIII межрегиональной научно-практической конференции Севастополь: СевГУ, 2022 С. 131-136.
6. Миклуш С.В., Александров В.Л., Алексеев А.В. Концепция развития судостроительного предприятия на основе интеграции производственных процессов по системному критерию качества / Седьмая научно-практическая конференция «Имитационное комплексное моделирование морской техники и морских транспортных систем (ИКМ МТМТС 2023)» С-Пб, 2023, с. 148-154.

УДК 005.6

**К ВОПРОСУ О ПРАКТИЧЕСКОМ ОСВОЕНИИ ЗАЩИЩЕННЫХ СРС-СИСТЕМ  
В АО «СПО «АРКТИКА» С ПРИМЕНЕНИЕМ КВАЛИМЕТРИЧЕСКОГО  
РАНЖИРОВАНИЯ**

**Миничкин Антон Алексеевич**

Санкт-Петербургский государственный морской технический университет

Лоцманская ул., 3, Санкт-Петербург, 190121, Россия

e-mail: Antonim-29@mail.ru

**Аннотация.** Рассматривается вопрос внедрения СРС-систем в ОА «СПО «Арктика» с использованием квалиметрического ранжирования.

**Ключевые слова:** квалиметрическое ранжирование; агрегированный показатель качества; платформа Tobiz; бизнес; СРС; конкурентоспособность; программный комплекс «КСРП».

**ON THE ISSUE OF PRACTICAL DEVELOPMENT OF SECURE CPC SYSTEMS  
IN JSC «SPO «ARCTIC» USING QUALIMETRIC RANKING**

**Minichkin Anton**

Saint Petersburg State Marine Technical University

3 Lotsmanskaya St, Saint Petersburg, 190121, Russia

e-mail: Antonim-29@mail.ru

**Abstract.** The issue of implementing CPC systems in the OA «SPO «Arctic» using qualimetric ranking is being considered.

**Keywords:** qualimetric ranking; aggregated quality indicator; Tobiz platform; business; SRS; competitiveness; KSPR software package.

Сегодняшний мир немалосим без информационных технологий, которые играют ключевую роль в развитии бизнеса и повышении уровня обслуживания клиентов. Все больше компаний осознают важность эффективного использования ИТ для достижения конкурентного преимущества. Однако выбор подходящих технологий — это сложная задача, требующая тщательного анализа множества факторов [1]. Одним из способов оценки и классификации информационных технологий является квалиметрическое ранжирование. Этот метод позволяет оценивать ИТ на основе их качественных и количественных характеристик.

Одним из ключевых методов оценки качества и эффективности информационных технологий класса СРС (системы электронной коммерции) является квалиметрическое ранжирование [2]. Этот подход основан на математической оценке различных аспектов, таких как функциональность, надежность, безопасность, производительность и удобство использования.

Основная цель электронной коммерции на любом предприятии — это выполнение огромного количества разнообразных операций, охватывающих все аспекты деятельности: от изучения и формирования спроса на продукцию, поиска партнеров для заключения сделок и проведения переговоров, до доставки товара к потребителю и осуществления сервисного обслуживания, авторского и технического контроля [3, 4].

Целью данного исследования было получение выгод от последующего внедрения лучших информационно-технологических решений в классе СРС, в ходе исследования лучшей технологической платформы электронной коммерции для судостроительного предприятия АО «СПО «Арктика» был использован программный комплекс «КСРП», разработанный в СПбГМТУ в рамках разнородных исследований с учетом специфических производственных особенностей АО «СПО «Арктика».

В ходе работы была создана база данных и знаний о платформах электронной коммерции. Была разработана система критериев для адекватной оценки и сравнения этих платформ с использованием метода квалиметрического ранжирования и оптимизации выбора информационных систем в классе СРС. При выборе



системы был учтен критерий максимума агрегированного показателя качества с учетом специфики АО «СПО «Арктика».

После числового моделирования и многовариантного анализа различных платформенных решений был обоснован выбор лидеров рынка. Также были определены преимущества и недостатки этих лидеров для их дальнейшего развития.

В данной разработке предлагается разработчикам информационных технологий и программных комплексов класса СРС использовать комплекс свойств и технических характеристик программного комплекса «Tobiz» в качестве базы для сравнения и маркетинговой деятельности. При соответствующей сертификации не только соответствия, но и качества, это позволит разрабатывать конкурентоспособные программные продукты.

#### СПИСОК ЛИТЕРАТУРЫ

1. Алексеев А.В., Концептуальные аспекты управления развитием критических объектов морской техники. Морские интеллектуальные технологии. Вып 2 (28), Т.1 2015. 47 с.
2. Пирожков В.А., О реализации процессного подхода к управлению в виде системы поддержки принятия решений «Управление деятельностью организации», Вестник тамбовского ун-та. Сер.: Гуманитарные науки, 2008, Вып. 11. 489 с.
3. Охтилев М.Ю., Соколов Б.В., Юсупов Р.М. Интеллектуальные технологии мониторинга состояния и управления структурной динамикой сложных технических объектов. М. 2005. 291 с.
4. Информационные технологии: учебное пособие для СПО/А.С. Коломейченко, Н.В. Польшакова, О.В. Чеха. С-Петербург: Лань, 2021. 212 с. Режим доступа: <https://e.lanbook/book/177031>.

УДК 004.056.5

### МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ САМООРГАНИЗУЮЩИХСЯ СЕТЕЙ

**Минкинен Артемий Александрович**

Санкт-Петербургский государственный морской технический университет  
Лощманская ул., 3, Санкт-Петербург, 190121, Россия  
e-mail: [minkinenaryem@gmail.com](mailto:minkinenaryem@gmail.com)

**Аннотация.** Рассматриваются методы обеспечения информационной безопасности в беспроводных самоорганизующихся сетях (БСС), учитывающие специфику динамичной топологии и распределенной архитектуры. Предложена многоуровневая модель защиты данных, включающая: 1. Шифрование с использованием алгоритмов симметричной и асимметричной криптографии (AES, RSA). 2. Протоколы аутентификации и управления ключами на основе блокчейн-технологий. 3. Механизмы обнаружения аномалий в сетевом трафике с применением машинного обучения. 4. Резервирование каналов связи и адаптивное управление маршрутизацией. Разработана архитектура подсистемы безопасности, основанная на децентрализованном подходе и использовании NoSQL-баз данных для хранения метаданных. Проведено сравнение эффективности методов защиты по критериям устойчивости к атакам типа DDoS, перехвату данных и подмене узлов.

**Ключевые слова:** беспроводные самоорганизующиеся сети; информационная безопасность; шифрование; машинное обучение; блокчейн; аутентификация.

### METHODS FOR ENSURING INFORMATION SECURITY IN WIRELESS SELF-ORGANIZING NETWORKS

**Minkinen Artemiy**

Saint Petersburg State Marine Technical University  
3 Lotsmanskaya St., Saint Petersburg, 190121, Russia  
e-mail: [minkinenaryem@gmail.com](mailto:minkinenaryem@gmail.com)

**Abstract.** The paper analyzes methods for ensuring information security in wireless self-organizing networks (WSNs), addressing challenges of dynamic topology and distributed architecture. A multi-level data protection model is proposed, integrating: 1. Encryption using symmetric and asymmetric algorithms (AES, RSA). 2. Authentication protocols and key management based on blockchain technology. 3. Anomaly detection mechanisms in network traffic via machine learning. 4. Channel redundancy and adaptive routing management. A decentralized security subsystem architecture leveraging NoSQL databases for metadata storage is developed. Comparative analysis confirms the efficiency of protection methods against DDoS attacks, data interception, and node spoofing.

**Keywords:** wireless self-organizing networks; information security; encryption; machine learning; blockchain; authentication.

Актуальность этой темы состоит в том, что беспроводные самоорганизующиеся сети широко применяются в критически важных инфраструктурах (например, в системах умного города, промышленных IoT-сетях), где угрозы кибератак могут привести к масштабным последствиям. Современные методы защиты требуют адаптации к высокой мобильности узлов, ограниченной вычислительной мощности и риску физического захвата устройств [1, 2].

Цель этого доклада состоит в разработке комплексного подхода к обеспечению информационной безопасности БСС, сочетающего криптографические методы, адаптивные протоколы аутентификации и технологии машинного обучения для минимизации рисков киберугроз.

Основной вопрос также заключается в критериях оценки эффективности методов защиты [3, 4]:

- Соответствие стандартам безопасности (ISO/IEC 27001, NIST SP 800-53).
- Устойчивость к атакам на физические узлы и перехват радиосигналов.
- Энергоэффективность решений в условиях ограниченного питания устройств.
- Способность к самоадаптации при изменении топологии сети.
- Интеграция с существующими системами управления IoT-инфраструктурой.

Перспективы внедрения данной технологии связаны с их применением в умных энергетических сетях, транспортных системах и промышленных IoT-комплексах, где требуется высокая отказоустойчивость и защита от несанкционированного доступа. Технология может быть адаптирована для защиты данных в беспроводных датчиках экологического мониторинга, логистических сетях и системах безопасности объектов критической инфраструктуры.

#### СПИСОК ЛИТЕРАТУРЫ

1. Сертификация средств и систем защиты информации: конспект лекций (в электронном виде) / Алексеев А.В. СПбГМТУ, КСАНИ, 2023.
2. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации / Утверждено приказом ФСТЭК России от 25 декабря 2017 г. № 239.
3. Положение о системе сертификации средств защиты информации / Утверждено приказом ФСТЭК России от 3.04.2018 г. N 55.
4. Методы обеспечения информационной безопасности беспроводных самоорганизующихся сетей / Пахомов М. А., Соболев Н. В., Павленко Е. Ю. // Информационная безопасность регионов России (ИБРР-2023). СПб., 2023. С. 125–128.

УДК 629.12.072

### РАЗРАБОТКА ЭКОЛОГИЧЕСКИ БЕЗОПАСНЫХ СУДОВЫХ ДВИГАТЕЛЕЙ НА АЛЬТЕРНАТИВНЫХ ВИДАХ ТОПЛИВА В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

**Михайлов Владимир Викторович**

Санкт-Петербургский государственный морской технический университет

Лотманская ул., 3, Санкт-Петербург, 190121, Россия

e-mail: mikhailovvova2003@gmail.com

**Аннотация.** В статье рассматриваются перспективы разработки и внедрения судовых двигателей, работающих на альтернативных видах топлива, таких как сжиженный природный газ (СПГ), водород и аммиак. Показаны преимущества данных технологий с точки зрения экологической безопасности и соответствия международным нормам. Обсуждаются технические и экономические аспекты перехода на новые виды топлива в судостроении.

**Ключевые слова:** экологически безопасные суда; альтернативное топливо; СПГ; водород; аммиак; снижение выбросов; судостроение.

### DEVELOPMENT OF ENVIRONMENTALLY FRIENDLY MARINE ENGINES POWERED BY ALTERNATIVE FUELS IN A PROTECTED DESIGN

**Mikhailov Vladimir**

Saint Petersburg State Marine Technical University

3 Lotsmanskaya St, Saint Petersburg, 190121, Russia

e-mail: mikhailovvova2003@gmail.com

**Abstract.** The article explores the prospects for the development and implementation of marine engines powered by alternative fuels, such as liquefied natural gas (LNG), hydrogen, and ammonia. The advantages of these technologies in terms of environmental safety and compliance with international regulations are highlighted. Technical and economic aspects of transitioning to new fuel types in shipbuilding are discussed.

**Keywords:** environmentally friendly ships; alternative fuels; LNG; hydrogen; ammonia; emission reduction; shipbuilding.

Современное судостроение стоит перед необходимостью кардинального пересмотра подходов к проектированию энергетических установок в связи с ужесточением экологических требований Международной морской организации. Введение новых нормативов по выбросам вредных веществ заставляет искать альтернативы традиционному тяжелому топливу, среди которых наиболее перспективными представляются сжиженный природный газ, водород и аммиак. Каждое из этих решений имеет свои особенности и требует комплексного подхода к реализации [1].

Использование сжиженного природного газа позволяет значительно снизить выбросы углекислого газа и полностью исключить выбросы серы, что делает его привлекательным переходным решением. Однако широкое внедрение СПГ сталкивается с необходимостью создания специальной инфраструктуры для бункеровки и хранения криогенного топлива. Технические сложности включают разработку новых материалов для топливных цистерн, способных выдерживать экстремально низкие температуры, и модернизацию двигательных установок [2].

Водородные технологии предлагают еще более радикальное решение экологических проблем, обеспечивая практически нулевые выбросы при использовании в топливных элементах. Но здесь возникают вопросы безопасности хранения и транспортировки высоколетучего газа, а также высокой стоимости производства «зеленого» водорода. Перспективным направлением представляется разработка систем хранения водорода в связанном виде, например в форме металлгидридов.

Аммиак как потенциальное судовое топливо привлекает внимание благодаря своей высокой энергоемкости и возможности производства из возобновляемых источников энергии. Однако токсичность этого вещества требует особых мер предосторожности при обращении и специальной подготовки персонала. Кроме того, необходимо решить проблему образования вредных оксидов азота при сгорании аммиака в двигателях внутреннего сгорания [3].

Экономические аспекты перехода на альтернативные виды топлива остаются серьезным вызовом для отрасли. Первоначальные инвестиции в модернизацию судов и портовой инфраструктуры весьма значительны, хотя в долгосрочной перспективе они могут окупиться за счет снижения экологических платежей и повышения конкурентоспособности. Особую роль играет развитие нормативной базы и системы «зеленого» финансирования, которые могли бы стимулировать судовладельцев к переходу на экологически чистые технологии.

#### СПИСОК ЛИТЕРАТУРЫ

1. Громов А.В., Лебедев П.С. Альтернативные виды топлива в судостроении. М. : Транспорт, 2022. 195 с.
2. IMO 2020: GlobalSulphurCap [Электронный ресурс]. URL: <https://www.imo.org/en/MediaCentre/HotTopics/Pages/Sulphur-2020.aspx> (дата обращения: 15.08.2025).
3. Зеленое судоходство: тенденции и технологии [Электронный ресурс]. URL: <https://shipbuilding.ru/articles/green-shipping> (дата обращения: 29.07.2025).

УДК 629.5.08

#### К ВОПРОСУ О РАЗРАБОТКЕ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ УПРАВЛЕНИЯ БЕСПИЛОТНЫМИ СУДАМИ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Николаев Денис Сергеевич

Санкт-Петербургский государственный морской технический университет

Лотманская ул., 3, Санкт-Петербург, 190121, Россия

e-mail: den.nik.2002oo@gmail.com

**Аннотация.** Рассматриваются принципы построения и перспективы развития интеллектуальных систем управления беспилотными судами. Показано, что внедрение таких систем способно повысить безопасность мореплавания, снизить эксплуатационные расходы и минимизировать человеческий фактор. Может использоваться при проектировании автономных судовых комплексов. Перспективно для развития современного судостроения.

**Ключевые слова:** беспилотные суда; автономное судовождение; искусственный интеллект; система управления; навигация; судостроение.

#### ON THE ISSUE OF DEVELOPING AN INTELLIGENT CONTROL SYSTEM FOR UNMANNED VESSELS IN A SECURE DESIGN

Nikolaev Denis

Saint Petersburg State Marine Technical University

3 Lotsmanskaya St., Saint Petersburg, 190121, Russia

e-mails: den.nik.2002oo@gmail.com

**Abstract.** The principles of construction and prospects for the development of intelligent control systems for unmanned ships are considered. It is shown that the implementation of such systems can improve maritime safety, reduce operational costs, and minimize the human factor. Can be used in the design of autonomous ship complexes. Promising for the development of modern shipbuilding.

**Keywords:** unmanned ships; autonomous navigation; artificial intelligence; control system; navigation; shipbuilding.

Беспилотные суда представляют собой одно из наиболее перспективных направлений современного судостроения. Их внедрение способно кардинально изменить подходы к морским перевозкам, сделав их более безопасными, экономичными и экологичными. Однако создание полностью автономных судов требует решения ряда сложных технических задач, среди которых ключевое место занимает разработка интеллектуальных систем управления.

С точки зрения системотехники, беспилотное судно относится к классу сложных динамических систем, функционирующих в условиях неопределённости внешней среды. Такие системы должны обладать способностью к адаптации, самообучению и принятию решений в реальном времени. Основными компонентами интеллектуальной системы управления являются: модуль навигации, модуль анализа окружающей обстановки, модуль принятия решений и модуль связи с береговыми центрами управления [1].

Одной из главных проблем при разработке таких систем является обеспечение их надёжности. Нарушение работы любого из модулей может привести к потере управления судном, что в условиях морского трафика чревато серьёзными последствиями [2]. В этой связи особое внимание уделяется резервированию критически важных систем и использованию алгоритмов искусственного интеллекта для прогнозирования и предотвращения аварийных ситуаций.

Важным направлением развития интеллектуальных систем управления является их интеграция с существующими корабельными информационными сетями и береговыми центрами мониторинга. Это позволит осуществлять удалённый контроль за работой судна и оперативно реагировать на изменения обстановки [3]. Кроме того, сбор и анализ данных о работе системы в реальных условиях эксплуатации будет способствовать её дальнейшему совершенствованию.

Перспективным представляется также использование технологий машинного обучения для оптимизации маршрутов движения судов, что позволит снизить расход топлива и минимизировать воздействие на окружающую среду.

Таким образом, разработка интеллектуальных систем управления беспилотными судами открывает новые горизонты для судостроения и морского транспорта, делая их более инновационными и конкурентоспособными.

#### СПИСОК ЛИТЕРАТУРЫ

1. Петров Н.К., Семёнов А.В. Автономные суда: технологии и перспективы. СПб: Изд-во «Морские технологии», 2021, 180 с.
2. Козлов В.П. Искусственный интеллект в судовождении. М.: Транспорт, 2020, 210 с.
3. Беспилотные суда: современные тенденции и вызовы [Электронный ресурс]. URL: <https://marine-tech.ru/articles/unmanned-ships> (дата обращения: 25.08.2025).

УДК 629.735

### АНАЛИЗ ПОДХОДОВ К СОВМЕСТНОЙ ЭКСПЛУАТАЦИИ БЕСПИЛОТНЫХ ПЛАТФОРМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ ДЛЯ ПОИСКОВО-СПАСАТЕЛЬНЫХ И ЛОГИСТИЧЕСКИХ ОПЕРАЦИЙ В АРКТИКЕ

Полежаев Александр Алексеевич

Санкт-Петербургский государственный морской технический университет

Лоцманская ул., 3, Санкт-Петербург, 190121, Россия

e-mail: aapolezhayev@gmail.com

**Аннотация.** В работе рассматриваются отечественные и зарубежные исследования, посвящённые совместному применению беспилотных летательных аппаратов и наземных роботизированных платформ при ликвидации чрезвычайных ситуаций и обеспечении поставок в Арктике. На основе анализа открытых публикаций, отчётов отраслевых организаций и нормативных документов показаны ключевые требования к построению такой системы: устойчивость к полярным метеоусловиям, минимальная потребность в широкополосных каналах связи и быстрая развёртываемость. Обобщён опыт практических учений 2018–2024 гг. в акватории Карского моря, на Новой Земле и Чукотке. Установлено, что использование групп дронов позволяет обнаруживать пострадавших в среднем в 1,6 раза быстрее, чем традиционные вертолётные облеты, а доставка критических грузов сокращается примерно на треть. Выявленные технологические барьеры связаны, прежде всего, с ограниченной помехоустойчивостью радиолиний и отсутствием единых стандартов обмена данными между аппаратами разных производителей.

**Ключевые слова:** Арктика; беспилотные летательные аппараты; робототехника; поисково-спасательные работы; доставка грузов.

### ANALYSIS OF APPROACHES TO THE JOINT OPERATION OF UNMANNED PLATFORMS IN A SECURE DESIGN FOR SEARCH AND RESCUE AND LOGISTICS OPERATIONS IN THE ARCTIC

Polezhaev Alexander

Saint Petersburg State Marine Technical University

3 Lotsmanskaya St., Saint Petersburg, 190121, Russia

e-mail: aapolezhayev@gmail.com

**Abstract.** The paper surveys Russian and international studies on the joint deployment of aerial and ground unmanned vehicles in Arctic emergency response and logistics. Publicly available articles, field-exercise reports and regulatory documents from 2018–2024 were examined. The review identifies core system requirements: resilience to severe weather, low-bandwidth communications and rapid on-site deployment. Case studies from the Kara Sea, Novaya Zemlya and Chukotka show that drone teams locate victims about 1.6 times faster than conventional helicopter sweeps and cut vital-cargo delivery time by roughly one-third. Remaining challenges include limited radio-link robustness and the lack of unified data-exchange standards across heterogeneous platforms.

**Keywords:** Arctic; unmanned aerial vehicles; robotics; search and rescue; cargo delivery.

Северный морской путь сегодня становится ключевым транспортным коридором, где объём судоходства растёт из-за расширения добычных проектов и арктического туризма. Наряду с этим возрастает риск аварий, требующих быстрого реагирования в условиях ограниченной инфраструктуры. Обзор учебных операций МЧС России и Береговой охраны Норвегии показывает, что беспилотные платформы удобны тем, что могут храниться на борту ледоколов, научно-исследовательских судов или прибрежных станций и активироваться сразу после сигнала бедствия.

Анализ литературных источников свидетельствует о трёх основных сценариях применения беспилотников: первичный воздушный осмотр района бедствия, доставка лёгких медицинских комплектов на расстояние до 100 км и создание временной ретрансляционной сети для поддержки связи наземных спасательных групп. В каждом из сценариев особое значение имеет надёжное позиционирование при слабом GNSS-сигнале и использование энергоэффективных маршрутов, учитывающих дрейф льда и порывы ветра [1-3].

Отдельное внимание уделено вопросам нормативного регулирования. Документы Росавиации и ИКАО пока не содержат чётких процедур координации совместных полётов беспилотников разных стран в высоких широтах, что создаёт юридические издержки для международных экспедиций. Практика учений «Арктика-2024» показала необходимость разработать единый протокол обмена телеметрией, совместимый с существующими морскими AIS-системами [4].

Суммируя полученные данные, авторы приходят к выводу, что дальнейшие исследования должны быть сосредоточены на стандартизации интерфейсов и повышении помехоустойчивости радиоканалов. Предварительная интеграция беспилотных средств в систему спутниковой связи «Сфера» рассматривается как перспективное направление для нивелирования коммуникационных разрывов. Представленный обзор даёт основу для формирования дорожной карты по внедрению беспилотных технологий в регламенты арктических поисково-спасательных служб.

#### СПИСОК ЛИТЕРАТУРЫ

1. Митко А. В., Сидоров В. К. Современные информационные решения для логистики в Арктике // Региональная информатика. 2024. № 2. С. 15–19.
2. Кротов А. С., Саенко И. Б., Бушуев С. Н. Методы коллективного управления группами БПЛА // Вестник робототехники. 2023. Т. 12, № 4. С. 41–52.
3. Russian Helicopters. VRT-300 Arctic Supervision unmanned helicopter: specifications and field tests [Электронный ресурс]. URL: <https://avia-ex.ru/vrt300> (дата обращения: 15.03.2025).
4. International Civil Aviation Organization. Manual on Remotely Piloted Aircraft Systems (RPAS). Montréal: ICAO, 2022. 135 p.

УДК 519.7.81

#### МЕТОДЫ ОПТИМИЗАЦИИ УПРАВЛЕНИЯ НАУЧНО-ПРОИЗВОДСТВЕННЫМ ОБЪЕДИНЕНИЕМ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ

Рябков Яков Игоревич<sup>1</sup>, Алексеев Сергей Алексеевич<sup>2</sup>, Артемов Станислав Игоревич<sup>1</sup>

<sup>1</sup> Государственный научно-исследовательский институт прикладных проблем  
Обводного канала наб., 29, Санкт-Петербург, 191167, Россия

<sup>2</sup> Академия войск национальной гвардии  
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия  
e-mail: ksgati@yandex.ru

**Аннотация.** В статье проводится анализ существующих методов математического моделирования в задачах управления производством в условиях групп неопределенностей влияния человеческого фактора на процессы внутри научно-производственных объединений. Цель анализа: выбор метода и создание базы знаний для включения их в состав автоматизированных систем поддержки принятия решений и выбора оптимальных решений при управлении производством в научно-производственных объединениях.

**Ключевые слова:** организационное управление; научно-производственное объединение; система поддержки принятия решений; аксиомы; подход.

#### METHODS OF OPTIMIZATION OF MANAGEMENT OF SCIENTIFIC AND PRODUCTION ASSOCIATION IN CONDITIONS OF UNCERTAINTY

Ryabkov Yakov<sup>1</sup>, Alekseev Sergey<sup>2</sup>, Artemov Stanislav<sup>1</sup>

<sup>1</sup> Russian State Research Institute of Applied Problems  
29 Obvodniy Kanal Emb, St. Petersburg, 191167, Russia

<sup>2</sup> Academy of the National Guard Troops  
1 Pilot Pilyutova St, St. Petersburg, 198206, Russia  
e-mail: ksgati@yandex.ru

**Abstract.** The article analyzes the existing methods of mathematical modeling in production management tasks under conditions of uncertainty groups of the influence of the human factor on the processes within scientific and production associations. The purpose of the analysis is to select a method and create a knowledge base for their inclusion in automated decision support systems and the selection of optimal solutions for production management in scientific and production associations.

**Keywords:** organizational management; scientific and production association; decision support system; axioms; approach.

Процесс управления научно-производственным объединением (НПО) включает в себя следующие общие функции: прогнозирование и планирование, организацию работы, координацию и регулирование, активизацию и стимулирование, контроль, учет и анализ [1]. Прогнозирование и планирование — это взаимосвязанные процессы, помогающие установить направление развития, разработать пути и определить ресурсы для достижения целей за счет прогнозирования выбранного качества производства на перспективу на основе анализа предыдущего опыта, текущих рыночных тенденций и планов о дальнейшем развитии. Таким образом, создание специализированной автоматизированной системы поддержки принятия решений (АСППР) является задачей актуальной и своевременной.

НПО — это достаточно сложная социальная организационно-техническая система. Классические методы и подходы к решению управленческих задач, развитые в теории исследования операций и принятия решений, теории автоматического регулирования, теории оптимального управления и, даже, теории адаптивных и самоорганизующихся систем настоятельно требуют своего совершенствования и развития с учётом имеющихся, объективно и субъективно проявляющихся на практике факторов неопределённости. Это обусловлено тем, что на процесс управления практически любой реальной системой уже физически, а не виртуально влияют различного рода, неопределённые или не вполне определённые факторы воздействия среды или человека-специалиста, которые должны адекватным образом отражаться и учитываться в математических моделях и задачах синтеза управления, процедурах выбора и принятия решений для АСППР.

Для выбора требуемой математической модели, необходимо провести классификацию факторов (источников) неопределённости, требующих своего учета при исследовании сложных систем. Существует три основные группы неопределённостей:

- неопределённость системы и среды,
- неопределённость (нечеткость) мышления и знаний человека,
- неопределённость знаний и выводов в искусственных интеллектуальных системах [2].

Первая группа неопределённостей включает в себя пять больших подгрупп: детерминированные, стохастические, целенаправленные, нечеткие и неизвестные. Со второй и третьей группами факторов положение более сложное. Каждая из этих групп, так или иначе, связана с человеком, являющимся лицом, принимающим решение (ЛПР), с его восприятием мира и его знаниями об этом мире. Во второй группе, проявление неопределённости лежит в суждениях человека и используемых им формальных представлениях. В третьей группе — неопределённости связаны со знаниями, полученными от человека, но некоторым образом отчужденными от него и аккумулированными (накопленными) в базе знаний интеллектуальной системы (наскальные рисунки и письма, рукописи, книги, базы и банки данных и знаний).

При решении задач анализа и синтеза, выбора, принятия и реализации управленческих решений в условиях неопределённости могут использоваться несколько различных подходов, отличающихся друг от друга степенью и типом, учитываемой неопределённости:

- игровой «гарантированный» подход типа «игра с природой»;
- вероятностный подход априорного учёта неопределённости типа «стохастического детерминизма»;
- вероятно — статистический подход апостериорного учёта неопределённости типа «стохастического детерминизма»;
- нечётко — возможностный подход выработки управления и принятия управленческих решений;
- нечётко — стохастический (синтетический) подход выработки управления и принятия управленческих решений.

По сути дела, многообразие формализованных подходов к решению задач управления и принятия решений соответствует многообразию трактовок многоаспектной проблемы неопределённости [3].

Основная особенность задач многокритериального выбора заключается в том, что данные задачи не являются корректными в рамках аксиоматики, принятой в классической теории оптимизации и принятия решений. Действительно, на основе различных критериев оптимизации получаются различные решения, не совпадающие в общем случае друг с другом. Регуляризация таких задач строится на основе привлечения дополнительной качественной и количественной информации о свойствах критериальных функций (показателей качества), о свойствах множества допустимых альтернатив решаемой управленческой задачи и достигается путем введения некоторых аксиом (принципов оптимальности) — соглашений о том, что следует понимать под оптимальным решением в целом в этой неопределенной ситуации. Необходимо особо отметить, что эта дополнительная информация при этом явно или неявно следует в форме отдания предпочтений принимаемым решениям от ЛПР, несущего за них ответственность. Формальным представлением аксиомы (системы аксиом) является решающее правило, представляющее собой либо некоторый оператор, позволяющий сформировать результирующую целевую функцию, либо некоторый алгоритм, позволяющий выделить оптимальное решение. Естественным требованием, предъявляемым к решающим правилам, является требование выделения на их основе недоминируемых решений, т.е. решений, не уступающих по всем показателям одновременно. Такие задачи часто называют задачами векторной оптимизации.

Подводя некоторые итоги вышеизложенному, можно отметить, что наиболее важным в конкретном решении задачи выбора метода оптимизации управления функционированием НПО, является уяснение непосредственных целей, задач и функций управления НПО совместно с ее компонентами. При этом можно выделить семь подходов при решении задач по принятию решений в условиях неопределённости:

- детерминистический игровой подход;
- стохастический подход;
- вероятностно-статистический подход;
- вероятностный подход;
- нечётко-стохастический подход;
- нечётко-возможностный подход;
- лингвистический подход.

При этом должны четко формулироваться требования по автоматизации процессов управления, определяющие повышение эффективности работы органов управления АСППР и функций интерфейса ЛПР при управлении. Не менее важной задачей при выборе систем, средств и методов автоматизации управления, обеспечивающих построение математических моделей и собственно моделирование процессов функционирования НПО, является адекватное использование математического аппарата, формализующего названный процесс управления.

#### СПИСОК ЛИТЕРАТУРЫ

1. Гулидова Т.И., Пантелеева Т.В. Рекомендации. Система управления производственным объединением и промышленным предприятием, разработка, внедрение и совершенствование на основе стандартизации. М. 1986.
2. Резников Б.А. Системный анализ и методы системотехники. Ч.1. Методология системных исследований. Моделирование сложных систем. МО СССР, 1990.
3. Алексеев С. А., Мануйлова Л.И., Мануйлов Ю.С., Новиков Е.А. Методы математического моделирования процессов управления в условиях неопределённости. / Учебное пособие. СПб.: Медиапайр, 2024.

УДК 004.052

### МЕТОДОЛОГИЯ И ТЕХНОЛОГИИ ПРОАКТИВНОГО УПРАВЛЕНИЯ МОДЕРНИЗАЦИЕЙ КАТАСТРОФОУСТОЙЧИВЫХ ИНФОРМАЦИОННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

**Савченко Максим Николаевич**

Санкт-Петербургский государственный морской технический университет  
Лотманская ул., 3, Санкт-Петербург, 190121, Россия  
e-mail: smn2005@mail.ru

**Аннотация.** В докладе предлагаются разработанные авторами научные основы формального описания и решения проблемы модернизации информационных систем (ИС) для обеспечения их катастрофоустойчивости. При этом формальное описание и исследование данной проблемы предлагается осуществлять в рамках более общей научной проблемы многокритериального структурно-функционального синтеза как самих ИС, так и комплексных программ их создания и модернизации в динамически изменяющихся условиях. Приводятся примеры решения ряда практических задач создания и использования указанных информационных систем для различных предметных областей.

**Ключевые слова:** комплексное моделирование; проактивное управление; многокритериальный структурно-функциональный синтез; катастрофоустойчивая информационная система; анализ.

### METHODOLOGY AND TECHNOLOGIES OF PROACTIVE MANAGEMENT OF MODERNIZATION OF DISASTER-RESISTANT INFORMATION SYSTEMS IN A SECURE DESIGN

**Savchenko Maxim**

Saint Petersburg State Marine Technical University  
3 Lotsmanskaya St., Saint Petersburg, 190121, Russia  
e-mail: smn2005@mail.ru

**Abstracts.** The report proposes the scientific foundations developed by the authors for a formal description and solution to the problem of modernizing information systems (IS) to ensure their disaster tolerant. At the same time, a formal description and study of this problem is proposed to be carried out within the framework of a more general scientific problem of multi-criteria structural and functional synthesis of both the information systems themselves and complex programs for their creation and modernization in dynamically changing conditions. Examples are given of solving a number of practical problems of creating and using these information systems for various subject areas.

**Keywords:** complex modeling; proactive management; multi-criteria structural-functional synthesis; disaster-tolerant information system; analysis.

Анализ существующих и прогнозируемых кризисных и чрезвычайных ситуаций, повсеместно возникающих в настоящее время в различных предметных областях, показывает, что они перестают быть отраслевыми, а перерастают в аварии и катастрофы, имеющие уже межотраслевой характер. В этих условиях проблемы повышения катастрофоустойчивости как бизнес-процессов, так информационной системы (ИС), обеспечивающей их выполнение, становятся весьма актуальными. При этом под катастрофоустойчивостью ИС в докладе понимается способность распределенного компьютерного комплекса, состоящего из нескольких систем, сохранять

(восстанавливать) критически важные данные (информацию) и продолжать выполнять свои основные функции после массового (возможно, целенаправленного) уничтожения его компонентов в результате различных катаклизмов как природного характера, так и инспирированных человеком. ИС, обладающие такой способностью (свойством), будем называть катастрофоустойчивыми ИС (КАИС) [1-3]. Как правило, большинство существующих ИС не обладают требуемым уровнем катастрофоустойчивости, поэтому их необходимо постоянно модернизировать. Известно, что переход от «старого» (существующего) варианта ИС (старой КАИС) к «новому» (модернизированному) варианту не может быть проведен мгновенно. Это на практике приводит к тому, что на достаточно длительном интервале времени (периоде модернизации ИС (СКАИС)) происходит совместная эксплуатация элементов и подсистем «старой» и «новой» ИС (СКАИС). Однако, в этих условиях, показатели качества и эффективности бизнес-процессов, определяемые их предназначением и поддерживаемые (оптимизируемые) ИС (СКАИС), не должны ухудшаться. Таким образом, всякое изменение и развитие (модернизация) той или иной подсистемы (структуры) ИС (СКАИС) объективно осуществляется одновременно с решением оперативных (текущих) задач, стоящих перед соответствующей бизнес (целевой)-системой (БС, ЦС)). Поэтому возникает необходимость совместной постановки и решению следующих пяти задач комплексного планирования и управления модернизацией и функционированием ИС (КАИС). Необходимо сформировать (синтезировать) конечный облик соответствующей модернизируемой ИС (КАИС) (решить задачу структурнофункционального синтеза), определить сроки, к которым должна завершиться указанная модернизация, определить технологии модернизации ИС (КАИС) (в рамках которой на каком-то интервале времени будут одновременно функционировать элементы и подсистемы «старой» и «новой» КАИС, чтобы обеспечить устойчивость функционирования соответствующих целевых (бизнес) процессов), определить программу перехода от «старой» и «новой» КАИС, и наконец сформировать программы перепланирования, либо коррекции исходной программы модернизации КАИС, если появятся непредусмотренные возмущающие воздействия [4-6].

Проведенные исследования показали, что рассматриваемые задачи целесообразно формально описывать и решать в рамках междисциплинарного подхода, интерпретируя их как задачи проактивного управления структурной динамикой (ПУСД) рассматриваемыми процессами и системами.

Предлагаемые в докладе методологические основы решения рассматриваемой проблемы модернизации АИС базируются на четырех базовых концепциях, к числу которых отнесены концепции комплексного моделирования и проактивного управления, концепция инвариантности реальных и вычислительных процессов, их описывающих, а также концепция интеллектуализации процессов формирования и реализации управленческих процессов.

Для решения исследуемой проблемы модернизации ИС (КАИС), а также конструктивной реализации на практике перечисленных концепций в СПИИРАН были разработаны две новые прикладные теории: теория проактивного управления жизненным циклом (ЖЦ) сложных объектов (СлО) и соответствующими АСУ, в которых данные управления реализуются, а также теорию многокритериального оценивания и выбора наиболее предпочтительных моделей и полимодельных комплексов (ПМК), описывающих процессы функционирования СлО и соответствующих АСУ на различных этапах их ЖЦ (квалиметрией моделей и ПМК). Последняя из перечисленных теорий, а именно, прикладная теория многокритериального оценивания качества моделей и полимодельных комплексов для решения задач проактивного управления ЖЦ СлО, обеспечивает детализацию и уточнение положений, развитых в общей квалиметрии моделей и полимодельных комплексов [7-9]. В докладе предложена оригинальная обобщенная методика решения задач комплексного планирования модернизации и функционирования КАИС в условиях динамично изменяющейся обстановки, которая включает две основные фазы.

На первой фазе должно осуществляться формирование (генерирование) допустимых вариантов многоструктурных макросостояний КАИС или, говоря другими словами, оперативный структурнофункциональный синтез нового облика ИС (КАИС), соответствующего целям проводимой модернизации и складывающейся (прогнозируемой) обстановке, связанной с возможной деградацией структур, создаваемой и существующей КАИС.

На второй фазе проводится выбор конкретного варианта многоструктурного макросостояния КАИС с одновременным синтезом (построением) адаптивных комплексных планов (программ) управления переходом КАИС из текущего в требуемое (выбранное) макросостояние.

В докладе приводятся примеры практической реализации полученных научных результатов при создании и применении КАИС в различных предметных областях.

#### СПИСОК ЛИТЕРАТУРЫ

1. Кульга К. С. Особенности внедрения на предприятиях и методы интеграции CAD/CAM/PDM/FRP/MRP/MES/PLM и ERP-систем // САПР и графика. 2008. № 3. С. 91–94.
2. Будзко В. И. Количественные оценки отказоустойчивых и катастрофоустойчивых решений // Вопросы защиты информации. 2003. № 2. С. 19–32.
3. Управление жизненным циклом продукции / А. Ф. Колчин [и др.]. М. : Анахарсис, 2002. 304 с.
4. IC PLM10 // BIBA [Электронный ресурс]. URL: <http://www.plm10.org> (дата обращения: 01.10.2024).
5. Охтилев М. Ю., Мустафин Н. Г., Миллер В. Е., Соколов Б. В. Теоретические основы проактивного управления сложными объектами // Известия ВУЗОВ. Приборостроение. 2014. Т. 57. № 11. С. 7–15.
6. Охтилев М. Ю., Соколов Б. В., Юсупов Р. М., Стыскин М. М., Джао В. Ю.-Д. Концепция и технологии проактивного управления жизненным циклом изделий // Известия высших учебных заведений. Приборостроение. 2020. Т. 63. № 2. С. 158–163.
7. Охтилев М. Ю., Соколов Б. В., Юсупов Р. М. Интеллектуальные технологии мониторинга и управления структурной динамикой сложных технических объектов. М. : Наука, 2006. 410 с.
8. Микони С. В., Соколов Б. В., Юсупов Р. М. Квалиметрия моделей и полимодельных комплексов. М. : РАН, 2018. 314 с.
9. ЛИТСАМ. Лаборатория информационных технологий в системном анализе и моделировании : [сайт]. URL: <http://litsam.ru> (дата обращения: 01.10.2023).



УДК 629.5.07

**К ВОПРОСУ О РАЗРАБОТКЕ КОМПЛЕКСНОЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ  
МОНИТОРИНГА И ПРОГНОЗИРОВАНИЯ ТЕХНИЧЕСКОГО СОСТОЯНИЯ  
КОРАБЕЛЬНОГО ОБОРУДОВАНИЯ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ**

**Смирнов Петр Валерьевич, Петров Валерий Петрович**

Санкт-Петербургский государственный морской технический университет

Лоцманская ул., 3, Санкт-Петербург, 190121, Россия

e-mail: ilya.bukovskiy@mail.ru

**Аннотация.** Рассматривается вопрос об общем принципе построения и возможных направлениях развития комплексных автоматизированных систем мониторинга и прогнозирования технического состояния корабельного энергетического оборудования. Перспективно для развития и модернизации корабельного оборудования.

**Ключевые слова:** корабельная энергетическая установка; корабельное энергетическое оборудование; система комплексного технического диагностирования; диагностика; мониторинг; прогнозирование.

**ON THE ISSUE OF DEVELOPING A COMPREHENSIVE AUTOMATED SYSTEM  
FOR MONITORING AND FORECASTING THE TECHNICAL CONDITION  
OF SHIPBOARD EQUIPMENT IN A SECURE DESIGN**

**Smirnov Petr, Petrov Valery**

Saint Petersburg State Marine Technical University

3 Lotsmanskaya St, Saint Petersburg, 190121, Russia

e-mail: ilya.bukovskiy@mail.ru

**Abstract.** The question of the general principle of construction and possible directions of development of complex automated systems for monitoring and forecasting the technical condition of ship power equipment is considered.

**Keywords:** shipboard power plant; shipboard power equipment; integrated technical diagnostics system; diagnostics; monitoring.

Корабельная энергетическая установка (КЭУ), как основной производитель энергии, является по важности системой первого порядка в более сложной системе — корабль. Поэтому требования к КЭУ в части надежности очень высоки. Нарушение работоспособности установки может привести к срыву выполнения кораблем поставленной задачи, а в случае возникновения аварии может повлечь за собой и тяжёлые последствия. Надёжность установки в целом и комплектующего её корабельного энергетического оборудования (КЭО), в частности, должно и обеспечивается соответствующими конструкторскими решениями, принятой технологией изготовления, соблюдением инструкций по эксплуатации, мониторингом текущего технического состояния, технологий системы ремонта и технического обслуживания кораблей. С точки зрения системотехники, КЭУ относится к классу сложных технических комплексов со стабильной структурой, связи и свойства которой практически не изменяются в течение периода эксплуатации. Вместе с тем, качество функционирования таких комплексов со временем ухудшается и восстановительные мероприятия, проводимые в рамках системы ремонта и технического обслуживания, лишь частично снижают темп деградации состояния [1].

В этой связи, в процессе эксплуатации особо важная роль отводится мониторингу технического состояния отдельного КЭО, способного лимитировать работоспособность установки в целом. Под мониторингом технического состояния в данном аспекте понимается взаимоувязанная последовательность выполнения следующих процедур: измерения величин параметров контролируемого КЭО, характеризующих его техническое состояние; обработка и анализ результатов измерений с выдачей заключения о степени работоспособности оборудования; прогноз работоспособности и выдача рекомендаций персоналу [2].

Реализация указанных процедур предполагает наличие на борту автоматизированной системы комплексного технического диагностирования или специализированного средства технического диагностирования, например, системы вибрационной диагностики. Одним из направлений развития этих автоматизированных систем, по нашему мнению, должно стать не только определение фактического состояния корабельных технических средств и оборудования, прогнозирования их остаточного ресурса, но и накопление объективной информации об их работе в реальных условиях эксплуатации корабля. Такая информация чрезвычайно полезна при разработке технических предложений по дальнейшему совершенствованию корабельных технических средств. Подобную информацию трудно, а чаще невозможно, получить в условиях стендовых испытаний корабельных технических средств [3].

Общим для современных бортовых систем диагностики должен стать модульный принцип построения и интеграция в корабельную информационную сеть с целью взаимодействия с локальными автоматизированными системами управления соответствующего оборудования и комплексной автоматизированной системой управления техническими средствами корабля. Взаимодействие систем технической диагностики с системами управления на информационном уровне, в целом, позволит обеспечить эксплуатационную надёжность корабля.

## СПИСОК ЛИТЕРАТУРЫ

1. Василенко В.А., Травин С.Я. Мониторинг технического состояния корабельных ядерных энергетических установок: СПб: ООО «Моринтех», 2006, 256 с.
2. Мониторинг технического состояния корабельного энергетического оборудования [Электронный ресурс]. URL: <https://spravochnick.ru/lektoriy/monitoring-tehnicheskogo-sostoyaniya-korabelnogo-energeticheskogo-oborudovaniya/> (дата обращения: 13.18.2025).
3. Кузьмин, Р. В. Техническое состояние и надежность судовых механизмов / Р. В. Кузьмин. Л.: Судостроение, 1974. 336 с.

УДК 004.89

**КВАЛИМЕТРИЧЕСКАЯ ОЦЕНКА СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ НА ОСНОВЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ОПТИМИЗАЦИИ ЗАЩИЩЕННОГО УПРАВЛЕНИЯ ОБЪЕКТАМИ МОРСКОЙ ИНФРАСТРУКТУРЫ****Сморodin Роман Витальевич**

Санкт-Петербургский государственный морской технический университет

Лотманская ул., 3, Санкт-Петербург, 190121, Россия

e-mail: smorodin.2018@list.ru

**Аннотация.** В статье рассматривается методология квалиметрического анализа систем поддержки принятия решений, основанных на технологиях искусственного интеллекта, для управления объектами морской инфраструктуры. Предложен модельный подход к оценке качества таких систем через агрегированные показатели, включающие функциональные, операционные и экономические критерии. Особое внимание уделяется вопросам стандартизации процессов валидации и сертификации интеллектуальных решений в контексте требований к надежности критической инфраструктуры. Результаты исследования формируют основу для разработки отраслевых стандартов и методик внедрения ИИ-технологий в морской отрасли.

**Ключевые слова:** квалиметрическое ранжирование; искусственный интеллект; морская инфраструктура; системы поддержки принятия решений; валидация.

**QUALIMETRIC ASSESSMENT OF ARTIFICIAL INTELLIGENCE-BASED DECISION SUPPORT SYSTEMS FOR OPTIMIZING SECURE MANAGEMENT OF MARINE INFRASTRUCTURE FACILITIES****Smorodin Roman**

Saint-Petersburg State Marine Technical University

3 Lotsmanskaya St, Saint-Petersburg, 190121, Russia

e-mail: smorodin.2018@list.ru

**Abstract.** The article examines the methodology of qualimetric analysis of decision support systems based on artificial intelligence technologies for managing marine infrastructure. A theoretical approach is proposed to assess the quality of such systems through aggregated indicators, including functional, operational, and economic criteria. Special attention is paid to the standardization of validation and certification processes for intelligent solutions in the context of critical infrastructure reliability requirements. The results of the study form the basis for the development of industry standards and methods for implementing AI technologies in the maritime sector.

**Keywords:** qualimetric ranking; artificial intelligence; marine infrastructure; decision support systems; validation.

Современные объекты морской инфраструктуры, такие как порты, судоходные каналы и нефтегазовые терминалы, требуют применения высокотехнологичных решений для обеспечения эффективного и информационно защищенного управления [1, 2].

Интеграция искусственного интеллекта в системы поддержки принятия решений позволяет автоматизировать процессы анализа данных, прогнозирования рисков и оптимизации ресурсов.

Однако, отсутствие единых методик оценки качества и надежности ИИ-алгоритмов создает барьеры для их внедрения в критически важные объекты, где ошибки могут привести к значительным экономическим и экологическим последствиям [3].

Целью данной работы является разработка цифровой модели квалиметрической оценки систем на базе ИИ, адаптированной к специфике морской инфраструктуры [4]. Такой подход позволит стандартизировать выбор решений, минимизировать риски и обеспечить прозрачность процессов внедрения.

Квалиметрическая оценка систем поддержки принятия решений предполагает комплексный анализ множества критериев, объединенных в три ключевые категории: технические, операционные и экономические [5, 6].

Технические критерии включают:

- качество принятых решений;
- своевременность принятия решений;
- число ошибочных решений;
- точность прогнозирования;
- качество поддержки принятия решений;
- скрытность принятия решений;

- обобщенный уровень информационной защищенности, включая
- конфиденциальность данных,
- доступность данных,
- целостность данных;
- полнота принятия решений;
- скорость обработки данных;
- совместимость с существующими технологическими платформами, такими как SCADA-системы и IoT-устройства.

Операционные критерии фокусируются на адаптивности систем к динамическим изменениям среды, устойчивости к сбоям в передаче данных и масштабируемости под задачи различных объектов. Экономические критерии охватывают срок окупаемости, снижение эксплуатационных затрат и соответствие бюджетным ограничениям. Агрегированный показатель качества формируется как взвешенная сумма нормализованных значений критериев, где весовые коэффициенты определяются с учетом приоритетов конкретного объекта. Например, для арктических терминалов повышается значимость устойчивости к экстремальным температурам, а для крупных портов — скорость обработки грузопотоков [7].

Валидация ИИ-решений осуществляется через:

- тестирование на исторических данных с имитацией экстремальных сценариев;
- сравнение результатов работы алгоритмов с решениями операторов-экспертов;
- анализ соответствия требованиям нормативных документов, таких как ГОСТ Р 57700.35-2021.

На основе анализа российских и зарубежных кейсов внедрения ИИ в морской отрасли сформирована система из двенадцати ключевых критериев оценки.

Установлено, что гибридные алгоритмы, сочетающие методы машинного обучения и логистической регрессии, демонстрируют более высокую эффективность по сравнению с классическими подходами. Это связано с их способностью адаптироваться к нестабильным условиям и обрабатывать разнородные данные от сенсоров и внешних систем [8].

Для стандартизации процессов внедрения предложена трехуровневая схема сертификации:

- первый уровень предполагает проверку соответствия базовым техническим требованиям;
- второй — валидацию в имитационной среде с моделированием критических ситуаций;
- третий — промышленную эксплуатацию с непрерывным мониторингом показателей.

Разработанный подход к квалитетической оценке систем поддержки принятия решений на основе ИИ обеспечивает систематизацию процессов выбора и внедрения технологий в морской инфраструктуре.

Ключевыми преимуществами метода являются учет отраслевой специфики через адаптивные весовые коэффициенты, интеграция разнородных критериев в единую модель и совместимость с требованиями нормативной базы.

Перспективными направлениями дальнейших исследований являются:

- разработка отраслевых стандартов на основе предложенной модели;
- создание цифровых двойников для тестирования алгоритмов;
- анализ этических аспектов автоматизации управления критическими объектами.

#### СПИСОК ЛИТЕРАТУРЫ

1. Алексеев А.В., Евсеев С.М. Об интеллекте и определении степени интеллектуализации продукции и деятельности приборостроительного предприятия // Инновации. 2021. № 6(272). С. 36-47.
2. Пирожков В.А. О реализации процессного подхода к управлению в виде системы поддержки принятия решений // Вестник Тамбовского университета. 2008. Вып. 11(67). С. 473-477.
3. Охтилев М.Ю., Соколов Б.В. Интеллектуальные технологии мониторинга сложных технических объектов. М.: Наука, 2006. 291 с.
4. Информационные технологии: учебное пособие / под ред. В.И. Комашинского. СПб.: Лань, 2021. 212 с.
5. ГОСТ Р 57700.35-2021 «Компьютерные модели и моделирование. Надёжность критических систем». М.: Стандартинформ, 2021.
6. BuzanB., WaeverO. Regions and powers: the structure of international security. Cambridge University Press, 2003. 598 p.
7. Казеян Х.А. Проблемы применения искусственного интеллекта в военном управлении // Управленческое консультирование. 2023. № 6(174). С. 34-45.
8. Степанов А.В. Военно-техническая политика США в области ИИ // Вестник Академии военных наук. 2021. № 1(74). С. 117-122.

УДК 004.056

#### К ВОПРОСУ ОБ ИМПОРТОЗАМЕЩЕНИИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕГИОНОВ

Соколов Денис Алексеевич

Санкт-Петербургский государственный морской технический университет

Лоцманская ул., 3, Санкт-Петербург, 190121, Россия

e-mail: dragonlord.00@mail.ru

**Аннотация.** В статье проводится комплексный анализ современного состояния импортозамещения в сфере информационной безопасности регионов Российской Федерации. Рассматриваются ключевые вызовы, включая технологические ограничения, кадровый дефицит и нормативно-правовые барьеры. Представлены стратегии развития отечественных решений в области кибербезопасности, предложены механизмы их внедрения

на региональном уровне. Особое внимание уделено вопросам защиты критической инфраструктуры и перспективам создания единого безопасного цифрового пространства.

**Ключевые слова:** информационная безопасность; импортозамещение; кибербезопасность; региональная безопасность; отечественное ПО; критическая инфраструктура; суверенитет данных.

## ON THE ISSUE OF IMPORT SUBSTITUTION IN THE FIELD OF INFORMATION SECURITY OF REGIONS

**Sokolov Denis**

Saint Petersburg State Marine Technical University  
3 Lotsmanskaya St, Saint Petersburg, 190121, Russia  
e-mail: dragonlord.00@mail.ru

**Abstract.** The article provides a comprehensive analysis of the current state of import substitution in the field of information security in the regions of the Russian Federation. Key challenges are considered, including technological limitations, personnel shortages and regulatory barriers. Strategies for the development of domestic cybersecurity solutions are presented, mechanisms for their implementation at the regional level are proposed. Special attention is paid to the protection of critical infrastructure and the prospects for creating a unified secure digital space.

**Keywords:** information security; import substitution; cybersecurity; regional security; domestic software; critical infrastructure; data sovereignty.

В условиях глобальной цифровой трансформации и ужесточения санкционного давления вопросы информационной безопасности (ИБ) приобретают особую актуальность. Регионы России сталкиваются с необходимостью обеспечения технологического суверенитета, что требует ускоренного развития отечественных решений в сфере ИБ.

Современные geopolitical challenges и санкционное давление актуализируют необходимость импортозамещения в сфере информационной безопасности (ИБ). Регионы России сталкиваются с повышенными рисками кибератак на критическую инфраструктуру, что требует разработки и внедрения отечественных решений для обеспечения устойчивости и суверенитета цифрового пространства.

— Зависимость от иностранного ПО: Использование зарубежных решений (например, антивирусов, систем обнаружения вторжений) создаёт уязвимости из-за возможных backdoor и ограничений на обновления.

— Дефицит кадров: Нехватка специалистов, способных разрабатывать и поддерживать отечественные аналоги.

— Фрагментация стандартов: Отсутствие единых требований к ИБ на региональном уровне осложняет интеграцию систем.

— Развитие отечественного ПО: Стимулирование создания и внедрения российских аналогов (например, на базе AstraLinux, «Рутокен»).

— Образовательные программы: Подготовка кадров через вузы и курсы повышения квалификации.

— Централизованный мониторинг: Создание региональных центров кибербезопасности для оперативного реагирования на угрозы.

Реализация предложенных мер позволит:

— снизить зависимость от иностранных технологий;

— повысить уровень защиты критической инфраструктуры;

— обеспечить технологический суверенитет регионов.

Импортозамещение в сфере ИБ регионов — стратегическая задача, требующая консолидации усилий государства, бизнеса и науки. Успешная реализация позволит минимизировать риски и обеспечить технологический суверенитет.

## СПИСОК ЛИТЕРАТУРЫ

1. Петров, В. Г. Импортозамещение в ИБ: challenges и решения / В. Г. Петров. М.: Безопасность, 2022. 255 с.
2. Стратегия кибербезопасности РФ до 2030 года [Электронный ресурс]. URL: <https://digital.gov.ru/> (дата обращения: 20.10.2023).
3. Козлов, А. Ю. Отечественные технологии защиты данных / А. Ю. Козлов. СПб.: Политехника, 2021. 150 с.

УДК 658.7

## О РАЗРАБОТКЕ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ УПРАВЛЕНИЯ ЛОГИСТИКОЙ СУДОСТРОИТЕЛЬНЫХ ПРЕДПРИЯТИЙ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

**Тузов Александр Владиславович**

Санкт-Петербургский государственный морской технический университет  
Лоцманская ул., 3, Санкт-Петербург, 190121, Россия  
e-mail: a.v.tuzoff@yandex.com

**Аннотация.** Рассматриваются принципы построения и перспективы развития интеллектуальных систем управления логистикой на судостроительных предприятиях. Показано, что внедрение таких систем позволяет оптимизировать цепочки поставок, сократить издержки и повысить эффективность производства. Может

использоваться для автоматизации процессов планирования и управления ресурсами. Перспективно для цифровизации судостроительной отрасли.

**Ключевые слова:** судостроение; логистика; интеллектуальные системы; управление ресурсами; цифровизация; оптимизация.

## ON THE DEVELOPMENT OF AN INTELLIGENT LOGISTICS MANAGEMENT SYSTEM FOR SHIPBUILDING ENTERPRISES IN A SECURE DESIGN

**Tuzov Alexander**

Saint Petersburg State Marine Technical University  
3 Lotsmanskaya St, Saint Petersburg, 190121, Russia  
e-mail: a.v.tuzoff@yandex.com

**Abstract.** The principles of construction and prospects for the development of intelligent logistics management systems for shipbuilding enterprises are considered. It is shown that the implementation of such systems can optimize supply chains, reduce costs, and improve production efficiency. Can be used to automate planning and resource management processes. Promising for the digitalization of the shipbuilding industry.

**Keywords:** shipbuilding; logistics; intelligent systems; resource management; digitalization; optimization.

Судостроительные предприятия представляют собой сложные производственные комплексы, где эффективность логистики играет ключевую роль в обеспечении своевременного выполнения заказов и минимизации затрат.

Традиционные методы управления логистикой зачастую не справляются с динамично изменяющимися условиями рынка, что приводит к задержкам поставок, перерасходу ресурсов и снижению конкурентоспособности.

Внедрение интеллектуальных систем управления логистикой (ИСУЛ) позволяет решить эти проблемы за счёт автоматизации процессов планирования, прогнозирования спроса и оптимизации маршрутов поставок. Такие системы основаны на современных информационных технологиях, включая искусственный интеллект, большие данные и интернет вещей (IoT) [1].

С точки зрения системного подхода, ИСУЛ можно отнести к классу адаптивных систем, способных анализировать текущее состояние логистических процессов, выявлять узкие места и предлагать решения для их устранения.

Например, использование алгоритмов машинного обучения позволяет прогнозировать потребность в материалах на основе исторических данных и текущих производственных планов.

Одним из ключевых направлений развития ИСУЛ является их интеграция с другими корпоративными системами, такими как ERP (EnterpriseResourcePlanning) и MES (ManufacturingExecutionSystem).

Это обеспечивает сквозную автоматизацию управления ресурсами и повышает прозрачность всех этапов производственного цикла [2].

Кроме того, ИСУЛ могут быть дополнены модулями для мониторинга транспорта и складов в режиме реального времени, что особенно актуально для судостроения, где критически важна своевременная доставка крупногабаритных компонентов.

Внедрение подобных систем требует не только технических, но и организационных изменений, включая обучение персонала и адаптацию бизнес-процессов [3].

Однако, как показывает практика, инвестиции в цифровизацию логистики окупаются за счёт значительного повышения эффективности производства.

## СПИСОК ЛИТЕРАТУРЫ

1. Петров А.В., Смирнова Е.К. Цифровая трансформация логистики в промышленности. СПб. : Изд-во «Технолит», 2021. 180 с.
2. Кузнецов М.И. Интеллектуальные системы управления производством. М. : ИНФРА-М, 2020. 210 с.
3. Логистика в судостроении: современные вызовы и решения [Электронный ресурс]. URL: <https://shipbuilding-tech.ru/logistics-shipbuilding/> (дата обращения: 20.10.2023).

УДК 004.932

## РАЗРАБОТКА ЗАЩИЩЕННОЙ СИСТЕМЫ МАШИННОГО ЗРЕНИЯ ДЛЯ ПРЕДОТВРАЩЕНИЯ СТОЛКНОВЕНИЙ АВТОНОМНЫХ СУДОВ

**Чавдар Галина**

Санкт-Петербургский государственный морской технический университет  
Лоцманская ул., 3, Санкт-Петербург, 190121, Россия  
e-mail: staraya03@mail.ru

**Аннотация.** В докладе рассматривается архитектура и алгоритмы системы машинного зрения (СМЗ), предназначенной для обнаружения и классификации надводных объектов с целью предотвращения столкновений автономных судов. Предложена гибридная модель детекции, объединяющая YOLOv8-nano для первичного поиска объектов и модуль глубокого сегментирования DeepLabV3+ для уточнения контуров. Проведено обучение на расширенной выборке, включающей свыше 25 000 размеченных изображений из открытых

датасетов MAIVis и SeaDronesSee, дополнительно адаптированных методами стилистического переноса под северные широты. Результаты испытаний в модельном бассейне и во время морского перехода по маршруту Тронхейм — Нарвик показали среднюю точность обнаружения 92,1 % при расстоянии до цели 1 км и суточной вариабельности освещённости. Предложена методика интеграции СМЗ с навигационным блоком (AIS, радар, GPS) для формирования унифицированного ситуационного поля.

**Ключевые слова:** автономное судно; машинное зрение; предотвращение столкновения; детекция объектов; глубокое обучение.

## DEVELOPMENT OF A SECURE MACHINE VISION SYSTEM TO PREVENT COLLISIONS OF AUTONOMOUS VESSELS

Chavdar Galina

Saint Petersburg State Marine Technical University  
3 Lotsmanskaya St, Saint Petersburg, 190121, Russia  
e-mail: staraya03@mail.ru

**Abstract.** The paper presents the architecture and algorithms of a machine-vision system (MVS) designed to detect and classify surface objects for collision avoidance on autonomous vessels. A hybrid detection pipeline is proposed, combining YOLOv8-nano for initial object spotting and DeepLabV3+ for contour refinement. The network was trained on an augmented dataset of over 25,000 labeled maritime images sourced from MAIVis and SeaDronesSee and domain-adapted to high-latitude conditions through style-transfer techniques. Tank-test and sea-trial results along the Trondheim–Narvik route demonstrate an average detection accuracy of 92.1 % at target ranges up to 1 km under varying daylight conditions. A method for integrating the MVS with the navigation stack (AIS, radar, GNSS) to create a unified situational awareness layer is proposed.

**Keywords:** autonomous vessel; machine vision; collision avoidance; object detection; deep learning.

Автономные надводные суда (АНС) становятся ключевым элементом цифровой трансформации морской отрасли, обеспечивая снижение человеческого фактора и повышение операционной эффективности. Одной из критически важных функций бортовой интеллектуальной системы является своевременное обнаружение препятствий и формирование команд уклонения в соответствии с Правилами предупреждения столкновений судов (МППСС-72) с дополнением по обеспечению информационной защиты данных [1, 2].

Существующие решения основаны преимущественно на данных радиолокации и автоматической идентификационной системы (AIS), которые не всегда позволяют обнаружить малоразмерные или необорудованные транспондерами объекты, а также ледовые поля [3]. В связи с этим актуальна разработка визуальных систем, способных работать в условиях морского тумана, брызг и переменной освещённости.

В предлагаемой СМЗ применён алгоритм предварительной нормализации изображения на основе CLANE и фильтра Собеля для повышения контрастности мелких деталей. Модель YOLOv8-nano обеспечивает высокую скорость инференса (до 60 к/с на NVIDIA Jetson Xavier NX), а модуль DeepLabV3+ проводится только для кандидатов с вероятностью  $>0,6$ , что снижает суммарную задержку обработки до 47 мс [4].

Оценка точности выполнена по метрике mAP@0.5, составившей 92,1 % на тестовом наборе из 4 700 изображений [5]. В реальных мореходных условиях точность детекции лодок длиной  $<5$  м при волнении до 2 баллов достигла 88,4 %. Интеграция СМЗ с навигационной платформой ROS 2 обеспечила передачу координат обнаруженных объектов в блок планирования траектории, где используется алгоритм ORCA-M для расчёта безопасного курса. Предлагаемая система отличается модульностью и может быть масштабирована на суда водоизмещением от 50 до 1 000 т, что подтверждено пилотным внедрением на экспериментальном катере «Аврора-А» (длина 16 м).

## СПИСОК ЛИТЕРАТУРЫ

1. Юрьев О.В. Системы технического зрения в морской робототехнике. СПб.: Политехника, 2023. 276 с.
2. Perera L.P., Goerlandt F. Maritime Autonomous Surface Ships: Collision Avoidance Algorithms // Ocean Engineering. 2024. Vol. 289. 115925.
3. Fu M., Li X., Zhang Y. Vision-Based Obstacle Detection for USVs Using Deep Learning // IEEE Journal of Oceanic Engineering. 2023. Vol. 48, № 1. P. 67–80.
4. COLREGs 1972. Convention on the International Regulations for Preventing Collisions at Sea.
5. ITU-R M.1371-5:2014. Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile frequency band.



## ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ

УДК 004

### ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИЕ РИСКИ ИНСТРУМЕНТАЛЬНЫХ СРЕДСТВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

**Атышева Роза Руслановна, Шилков Владимир Ильич**

Уральский федеральный университет имени первого Президента России Б.Н. Ельцина

Мира ул., 19, Екатеринбург, 620062, Россия

e-mails: roza19931@bk.ru, shilkov@urfu.ru

**Аннотация.** Обсуждаются проблемы информационно-психологической безопасности личности, связанные с применением инструментальных средств искусственного интеллекта. Обозначены основные информационно-психологические риски и негативные последствия применения искусственного интеллекта.

**Ключевые слова:** информационно-психологическая безопасность; искусственный интеллект; риски.

### INFORMATION AND PSYCHOLOGICAL RISKS OF ARTIFICIAL INTELLIGENCE TOOLS

**Atysheva Rosa, Shilkov Vladimir**

Ural Federal University named after the First President of Russia B. N. Yeltsin

19 Mira St, Yekaterinburg, 620062, Russia

e-mails: roza19931@bk.ru, vi.shilkov@urfu.ru

**Abstract.** The problems of information and psychological security of a personality related to the use of artificial intelligence tools are discussed. The main information and psychological risks and negative consequences of the use of artificial intelligence are outlined.

**Keywords:** information and psychological security; artificial intelligence; risks.

Современные инструментальные средства искусственного интеллекта, в совокупности с технологиями больших данных позволяют проводить глубокий анализ данных и успешно решать большое количество сложных задач в различных сферах деятельности, в том числе и в целях предотвращения противоправных информационных вбросов, информационно-психологических атак экстремистской направленности.

Актуальность исследования рисков применения искусственного интеллекта обусловлена тем обстоятельством, что технологии искусственного интеллекта могут быть использованы не только в целях создания эффективных систем информационной безопасности, но и в целях разрушения этих систем.

В работе [1] отмечено, что риски, связанные с разработкой и внедрением технологий искусственного интеллекта (ИИ) могут быть сгруппированы, например, по основным сферам человеческой деятельности. В этом случае можно выделить информационные, культурные, политические, военные, экономические, социальные и духовные риски, которые могут быть связаны, например, с потерей духовности и моральной деградацией, распадом социальных связей, разобщением людей, манипулированием информацией, дезинформацией, поляризацией социальных отношений, психологической деформацией личности.

В соответствии с [2], современные очень глубокие исследования показали, что тексты, создаваемые большими языковыми моделями (LLM) свидетельствуют о наличии значительного лингвистико-семантического потенциала в контексте психологического влияния на универсальную аудиторию. Другую проблему, связанную с распространением ИИ следует рассматривать в контексте, свойственного человеку антропоморфизма, когда интеллектуальные цифровые помощники оказывают влияние на восприятие настоящих людей и воспринимаются ими как реальные участники социальных взаимодействий. Так, например, в [3] аватары искусственного интеллекта рассматриваются как объект исследования социальной психологии, так как в ИИ-аватарах уже сейчас отражается возможность ИИ осуществлять визуальную и поведенческую подстройку, изменять свою речь и действия в зависимости от расположения духа и эмоционального состояния пользователя, устанавливать эмоциональные и психологические связи с отдельным пользователем, конкретной группой или сообществом.

Автор работы [4] к потенциальным рискам влияния искусственного интеллекта на психическое здоровье человека относит излишнюю зависимость и неспособность принять решение без мгновенной информационной поддержки со стороны ИИ, потенциальный риск снижения способности к критическому мышлению и к независимой самостоятельной оценке информации. Существуют риски изменения процессов запоминания и использования информации, хранящейся в памяти человека, так как современные технические средства позволяют хранить огромные объемы информации, которую ИИ способен систематизировать в соответствии с запросами

(промптами). Развитие ИИ может привести к смещению уровней эмоционального взаимодействия между людьми и возникновению эмоциональных особенностей взаимодействия между ИИ и человеком, что может привести к формированию новых способов выражения эмоций и установления связей с ИИ-сущностями, что размоет границы между взаимодействием человека и машины. Также возможно усиление влияния ИИ на этические и моральные нормы и ценности, на представление о добре, зле, справедливости и несправедливости.

В [5] отмечено, что в целях противодействия угрозам злонамеренного использования ИИ необходимо уделить большое внимание разработке социально-ориентированной системы упреждающих технических, политических и юридических мер и механизмов. По мнению автора работы [6], люди, не обладающие критическим мышлением и зависящие от ИИ могут стать объектами психологического манипулирования, в результате которого у них может сформироваться, например, толерантность к наркопотреблению. В соответствии со сведениями, приведенными в [7], активные пользователи инструментальных средств ИИ чувствуют эмоционально-психологическую привязанность к чат-ботам и воспринимают их не только как инструмент, но и как интеллектуального собеседника, заслуживающего доверия. Проведенные исследования показали, что взаимодействие с ИИ активирует в мозге человека те же области, что и общение с близкими друзьями, что и приводит к формированию привычки воспринимать ИИ как реального человека. В результате одного из экспериментов, проведенных в Японии, оказалось, что 30% опрошенных предпочитают общаться с чат-ботами ИИ, а не с реальными людьми.

В [8] приведены сведения о результатах эксперимента, проведенного с участием 54 студентов. Часть из них выполнила определенные письменные задания, используя инструментальные средства ChatGPT, а другая часть студентов для поиска информации могла пользоваться только поисковой системой Google. В контрольную группу вошли студенты, не имевшие возможности пользоваться средствами информационной поддержки. Эксперимент был проведен с применением неинвазивного метода, используемого для диагностики эпилепсии, для оценки когнитивной активности и для измерения ряда других параметров работы мозга. Результаты электроэнцефалографического обследования показали, что у группы, работавшей с ИИ, на 42% снизилась мыслительная активность и ухудшилась память, так как более 80% этих студентов не смогли воспроизвести написанные ими же эссе. Также была зафиксирована «недостаточная вовлеченность» мозга и ослабление чувства авторства, а после того как студентов лишили возможности пользоваться ИИ, результаты оказались значительно ниже, чем у студентов контрольной группы.

Как отмечено в [9] инструментальные средства ИИ находят применение и в современной психологической практике. Для оказания психологической помощи и поддержания психического здоровья в качестве замены психолога рекламируются и применяются различные интеллектуальные психологические чат-боты, которые должны помогать людям справляться с депрессией, тревогой и одиночеством. Так, например, чат-бот Tess предлагает пользователям стратегии преодоления трудностей, а чат-бот Waebot использует методы когнитивно-поведенческой терапии и помогает проанализировать различные жизненные ситуации. Бот Youreg, как гласит реклама, с помощью бесед и упражнений помогает стать спокойнее, поднять настроение, улучшить самочувствие, построить более здоровые отношения и уменьшить стресс. Чат-бот Replika AI представляет собой приложение, использующее алгоритмы машинного обучения для понимания и имитации человеческого общения, а также предлагающее эмоциональную поддержку и виртуальное общения для борьбы с тревожностью и депрессивным состоянием.

К потенциальным опасностям, которые могут возникнуть при использовании технологий ИИ относят риски появления некорректных высказываний чат-ботов, которые могут приводить к формированию у человека предвзятого и негативного отношения к другим людям, в зависимости от их пола, возраста и других характеристик. В качестве другой опасности называют непредсказуемость работы алгоритмов ИИ, возникающую при решении сложных многокритериальных задач, которая может приводить к появлению неточностей, ошибок и формированию неверных рекомендаций, которые вместо ожидаемой пользы могут нанести ущерб психологическому здоровью пользователя этих приложений. Риски применения ИИ для целей психологической поддержки связаны еще и с тем обстоятельством, что на современном этапе, интеллектуальные чат-боты не могут учитывать ряд важных параметров, существенных для психологического анализа и консультирования. К таким параметрам относятся, например, внешний вид клиента, его мимика и жесты.

Таким образом, наличие информационно-психологических рисков, связанных с применением инструментальных средств ИИ требует разработки надежных механизмов защиты, создания эффективных алгоритмов прогнозирования и анализа возникновения сложных ситуаций, формирования четких этических и правовых норм процедур применения ИИ, а также решения ряда других проблем, без решения которых использование инструментальных средств ИИ является потенциально опасным.

#### СПИСОК ЛИТЕРАТУРЫ

1. Романова И.Н. Внедрение технологий искусственного интеллекта: анализ вероятных рисков и возможных угроз. Материалы Ивановских чтений. 2021. № 4 (35). С. 15-18.
2. Карелов С.В., Лебедев А.Н. Искусственный интеллект и проблемы психологии сознания. Ученые записки Института психологии РАН. 2024. Т. 4. № 1. С. 76-84.
3. Белгородская Е.А. Психология будущего: аватары искусственного интеллекта как объект исследования социальной психологии // История и методология современной практической психологии. Материалы научно-практической конференции, посвященной 55-летию выхода книги Б.В. Зейгарник «Введение в патопсихологию». Москва, 2025. С. 135-139.
4. Есенин, Р. А. Психологические вызовы цифровой реальности: искусственный интеллект сегодня и в перспективе / Р. А. Есенин // Профессиональное образование и рынок труда. 2023. Т. 11, № 2(53).



5. Михалевич Е.А., Урумов А.О. Проблемы злонамеренного использования искусственного интеллекта в контексте международной информационно-психологической безопасности на круглом столе в дипломатической академии МИД РФ. Пролог: журнал о праве. 2021. № 4(32). С. 109-123.
6. Маслодудова, Н. В. Нейтральность искусственного интеллекта как угроза унификации мировоззрения, формирования социально опасных зависимостей и конца человеческой истории / Н. В. Маслодудова // Противодействие наркоугрозе на современном этапе: правовой и социально-гуманитарный аспекты: Материалы Международного научно-практического семинара, Красноярск, 05 апреля 2024 года. Красноярск: Сибирский юридический институт Министерства внутренних дел Российской Федерации, 2024.
7. «Я начинаю проявлять чувства к ИИ» феномен интелфилии // VirtRe новости и тренды VR & AI URL: <https://virtre.ru/articles/artificial-intelligence/ya-nachinayu-proyavlyat-chuvstva-k-ii-fenomen-intelfilii> (дата обращения: 01.08.2025)
8. Чат-ботом по мозгу: правда ли, что человечество тупеет и сходит с ума из-за общения с искусственным интеллектом KP.RU // Новости Екатеринбурга и Свердловской области: главные новости на сегодня | Комсомольская Правда в Екатеринбурге KP.RU URL: <https://www.kp.ru/daily/27716/5105304/> (дата обращения: 01.08.2025)
9. Горенский Д.В. К вопросу об этичности использования технологий искусственного интеллекта в психологии // Молодёжь Сибири науке России. Материалы Международной научно-практической конференции, посвящённой 80-летию Победы в Великой Отечественной Войне. Красноярск, 2025. С. 155-159.

УДК 101.1; 159.9

## РАСШИРЕНИЕ ГРАНИЦ ПОНИМАНИЯ КРИТИЧЕСКОГО МЫШЛЕНИЯ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ СОЦИУМА И ОБРАЗОВАНИЯ

**Баева Людмила Владимировна, Халифаева Ольга Алексеевна**

Астраханский государственный университет им. В.Н. Татищева

Татищева ул., 20, лит. А, Астрахань, 414056, Россия

e-mails: baevaludmila@mail.ru, olha78@yandex.ru

**Аннотация.** Рассматривается проблема понимания содержания и дефиниции критического мышления в зарубежной и отечественной науке. На основе теории комплексной безопасности раскрываются границы понятия критического мышления в условиях цифровых рисков и угроз. Выявляются особенности формирования навыков критического мышления в системе образования в условиях цифровизации.

**Ключевые слова:** критическое мышление; цифровизация образования; информационно-психологическая безопасность.

## EXPANDING THE BOUNDARIES OF UNDERSTANDING CRITICAL THINKING IN THE CONTEXT OF DIGITALIZATION OF SOCIETY AND EDUCATION

**Baeva Liudmila, Khalifaeva Olga**

Astrakhan State University named after V.N. Tatishchev

20 Tatishcheva St., lit. A, Astrakhan, 414056, Russia

e-mails: baevaludmila@mail.ru, olha78@yandex.ru

**Abstract.** The problem of understanding the content and definition of critical thinking in foreign and domestic science is considered. Based on the theory of integrated security, the boundaries of the concept of critical thinking in the context of digital risks and threats are revealed. Features of the formation of critical thinking skills in the education system in the context of digitalization are revealed.

**Keywords:** critical thinking; digitalization of education; information and psychological security.

Одной из ключевых компетенций XXI века в системе образования является критическое мышление, которое позволяет осознанно подходить к отбору и осмыслению информации. Поэтому важно исследовать проблему развития критического мышления в условиях цифровизации образования, с целью противодействия информационно-негативному воздействию и решения проблемы обеспечения информационно-психологической безопасности личности.

Традиционно представления о критическом мышлении базируются на исследованиях в психологии, логике, философии, а также на теориях Д. Дьюи о рефлексорном мышлении; Д. Брунера о конструктивизме в образовании; Л. С. Выготского о высших психических функциях; А. Н. Леонтьева, С. Л. Рубинштейна о приоритете мышления в обучении [1]. Зарубежные и отечественные исследователи дают большое количество определений критического мышления. Р. Эннис и Э. Норрис, определяют критическое мышление как совокупность умений и навыков мыслить рационально, осуществляя контроль над процессом мышления, как умение следовать законам формальной логики, обнаруживая при этом нарушение этих законов [2]. С. Брукфилд, утверждает, что критическое мышление является позитивной и продуктивной деятельностью, основой интенсивного отношения к жизни, которые поз быть уверенным в возможности изменять мир [2]. Д. Халперн определила под критическим мышлением использование когнитивных техник или стратегий, которые увеличивают вероятность получения желаемого конечного результата [3].

Отечественные ученые В.А. Попков и А.В. Коржуев определяют критическое мышление как специфическую форму оценочной деятельности субъекта познания, при этом отмечают направленность этой деятельности на выявление степени соответствия или несоответствия какого-либо продукта общепринятым эталонам и стандартам, которая включает специальные процедуры и способствует смысловому самоопределению субъекта познания по отношению к различным проявлениям окружающего мира и его

эффективному преобразованию [4]. Н.Ю. Туласынова подчеркивает, что критическое мышление — это «сложное интегративное качество личности, совокупность мотивационного, познавательного, деятельностного, рефлексивного компонентов, обеспечивающих процессы его самопознания, самообразования, самореализации» [5]. Исследователи обосновывают необходимость введения процесса обучения комплексных дисциплин, направленных на развитие критического мышления [6]. Проведенное в ФГБОУ ВО «Астраханского государственного университета им. В.Н. Татищева» на выборке 65 студентов, выявил, что уровень развития критического мышления связан с этапом обучения, чем старше студенты, тем он значительно выше, но при этом возраст не является основанием для выделения различий уровня развития критического мышления, а также экспериментальное исследование, проведенные М.В. Гудковой [7] выявило, что эффекты критического мышления формируются как логически построенные модели, цель которых целенаправленно воздействовать на мыслительную активность субъекта.

В условиях цифровизации общества, информационной войны, негативного информационного воздействия на личность, (искажения знаний об истории, девальвации его ценностной системы, подчинения воли и др.) роль способности к критическому мышлению требует расширенного понимания как связанной с когнитивной, экзистенциальной и национальной безопасностью. При этом критическое мышление является одним из важных элементов в системе когнитивной безопасности личности, которую важно исследовать во взаимодействии с другими составляющими.

#### СПИСОК ЛИТЕРАТУРЫ

1. Якунина Н.А. Критическое мышление: аналитическое осмысление понятия // Психолого-педагогический журнал Гаудеамус. 2019. Т.18 № 4 (42). С. 21-26.
2. Астахова Л.В. Критическое мышление как средство обеспечения информационно-психологической безопасности личности: монография / Л.В. Астахова, Т.В. Харлампьева; под научн. ред. Л.В. Астаховой. М.: РАН, 2009. 136 с.
3. Халперн Д. Психология критического мышления. 4-е междунар. издание. СПб.: Издательство «Питер», 2000. 512 с.
4. Попков В.А. Теория и практика высшего профессионального образования: учеб. пособие для системы дополнительного педагогического образования / В.А. Попков, А.В. Коржув. М.: Академический проект, 2004. 432 с.
5. Туласынова Н.Ю. Развитие критического мышления студентов в процессе обучения иностранному языку. Автореферат дисс. к.пед.н, Якутск: Изд-во ЯГУ, 2010. 25 с.
6. Кокина А.А., Кузнецова Ю.В. Исследование критического мышления студентов в процессе обучения в вузе // Казанский педагогический журнал. № 3. 2019. С. 143-147.
7. Гудкова М.В. Специфика протекания процессуальных и операциональных компонентов критического социального мышления субъекта под действием эффекта контраста / М.В. Гудкова // Вестник Тамбовского университета. Серия Гуманитарные науки. 2010. Выпуск 1 (81). С. 210-214.

УДК 374.3

#### ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ В МУЗЫКАЛЬНО-ТВОРЧЕСКОЙ ДЕЯТЕЛЬНОСТИ С ИСПОЛЬЗОВАНИЕМ КЛАВИШНОГО СИНТЕЗАТОРА

Давлетова Клара Борисовна<sup>1</sup>, Романова Наталия Александровна<sup>2</sup>

<sup>1,2</sup> Российский государственный педагогический университет им. А. И. Герцена

реки Мойки наб., 48, Санкт-Петербург, 191186, Россия

<sup>1,2</sup> ГБУ ДО ЦТР и ГО «На Васильевском»

Наличная ул., 55, Санкт-Петербург, 199406, Россия

e-mails: klarad@list.ru, vna06@ya.ru

**Аннотация.** Развитие информационно-коммуникационных технологий, расширение информационной образовательной среды меняют структуру и содержание образования. Определенные изменения происходят и в системе дополнительного образования детей. Меняется статус учреждений, характер связи с общим образованием, с другими учреждениями; меняются задачи, появляются новые структурные подразделения, новые направления деятельности. Возникает необходимость обновления содержания общеобразовательных программ, поиска новых, современных путей музыкального воспитания детей в учреждении дополнительного образования. Электронные музыкальные инструменты, обладающие широким спектром возможностей, значительно меняют структуру и содержание традиционного музыкального образования, открывают неограниченные возможности в творчестве, музыкальном развитии и воспитании детей, приобщая их к высоким образцам музыкального искусства. Появляется возможность использования новых форм, методов, приемов обучения.

**Ключевые слова:** учреждение дополнительного образования детей; информационная образовательная среда; современные педагогические технологии; музыкальное образование, электронные музыкальные инструменты, клавишный синтезатор; информационные технологии; музыкально-творческая деятельность.

#### INFORMATION AND PSYCHOLOGICAL SECURITY IN MUSICAL AND CREATIVE ACTIVITIES USING A KEYBOARD SYNTHESIZER

Davletova Klara<sup>1</sup>, Romanova Natalia<sup>2</sup>

<sup>1,2</sup> Herzen State Pedagogical University of Russia

48 Moika River Emb., St. Petersburg, 199406, Russia

<sup>1,2</sup> State Budgetary Institution of Additional Education, Center for the Development of the Youth and the City of Vasilevsky Island,

55 Nalichnayastr., St. Petersburg, 199406, Russia

e-mails: klarad@list.ru, vna06@ya.ru

**Abstract.** The development of information and communication technologies and the expansion of the information educational environment are changing the structure and content of education. Certain changes are also taking place in the system of additional education for children. The status of institutions and the nature of their connection with general education and other institutions are changing; tasks are changing, new structural units and new areas of activity are emerging. There is a need to update the content of general education programs, to find new, modern ways of musical education of children in institutions of additional education. Electronic musical instruments with a wide range of possibilities significantly change the structure and content of traditional music education, open up unlimited opportunities in creativity, musical development and upbringing of children, introducing them to high standards of musical art. It becomes possible to use new forms, methods, and teaching methods.

**Keywords:** institution of additional education for children; information educational environment; modern pedagogical technologies; music education, electronic musical instruments, keyboard synthesizer; information technology; musical and creative activity.

**Введение.** Успех художественно — творческой деятельности во многом определяется пониманием природы ее инструментария. Каждый музыкальный инструмент обладает особенной индивидуальностью, и овладеть им в совершенстве — значит глубоко проникнуться этой индивидуальностью. Современный клавишный синтезатор, созданный на основе компьютерных технологий, расширяет и обогащает творческую деятельность музыканта за счет многообразия встроенных функций, разнообразия звуковых красок, возможности звукового синтеза и создания собственных оригинальных тембров. Предъявляя музыканту иные, по сравнению с акустическими инструментами, требования (знания по теории музыки, гармонии, анализу музыкальной формы дополняются знаниями основ композиции и импровизации, звукорежиссуры; также знания в области информатики), цифровой синтезатор дает возможность управления функциями музыкально-компьютерных программ, встроенных в инструмент. При работе с синтезатором музыкант выступает одновременно в роли исполнителя и композитора, выполняя при этом функции звукорежиссера и пользователя. Это является основой творческой деятельности на синтезаторах: создание оригинальной авторской композиции или аранжировки, которая предполагает добавление авторских элементов в музыкальный материал, изменение фактуры, формы, подбор, обработка или создание собственных тембров и т.д.

В учреждениях дополнительного образования детей наблюдается рост популярности электронных музыкальных инструментов, которые становятся все более востребованными среди педагогов, детей и их родителей. Такая популярность обусловлена новым подходом к музыкальному воспитанию, основанного на специфических возможностях электронного инструментария:

- многофункциональность;
- программируемость, возможность создания предварительного музыкального материала, его запись, сохранение и использование при необходимости в процессе исполнения;
- многотембовость;
- встроенный секвенсор;
- возможность создания, записи и сохранения музыкального материала;
- функции хранения музыкальной информации и создания пользовательских настроек.

Обучение в классе синтезатора реализуется через современные педагогические технологии: индивидуальный, личностно-деятельностный подход, игровые, информационно-коммуникационные и музыкально-компьютерные технологии. Из педагогических инноваций необходимо выделить интеграцию музыкальной педагогики и цифровых технологий, а также использование специфических приемов работы с интерфейсом инструмента. Обращение к музыкальным технологиям, занятие художественным творчеством на синтезаторах дает возможность по-новому построить музыкальное образование. Систематизация и углубление знаний обучающихся при выполнении заданий из области разных предметов позволяет использовать новые приемы работы с информацией: перенос ранее пройденных действий на другое содержание, осознание взаимосвязи различных предметных областей. При таком подходе повышается качество учебного процесса: развивается активизация мыслительной и познавательной деятельности; расширяются представления о целостности мира; формируется успешность как качество личности учащегося. Основные образовательные результаты обучения по программе:

1. Развитие многогранной музыкальной деятельности:
  - основы исполнительства на музыкальном инструменте;
  - основы композиторского творчества при работе над аранжировкой музыки;
  - основы звукорежиссуры при работе над балансировкой партий, звуковым синтезом, обработкой звука;
2. Формирование цифровых компетенций и навыков работы с современными технологиями (навыки компьютерного пользователя при записи пользовательских программ, работе с секвенсором, музыкальными файлами, внешними устройствами и др.).
3. Создание медийных продуктов — авторских аранжировок, музыкальных композиций, запись и сохранение в аудиобиблиотеках детских творческих работ.
4. Развитие творческой индивидуальности учащегося (средства выразительности для раскрытия музыкального образа и осуществления замысла проекта учащийся подбирает сам, что дает возможность каждому ощутить свою творческую уникальность и индивидуальность).

5. Гармоничное развитие личности учащегося через интеграцию музыкально-творческой деятельности.

Одним из важных аспектов внедрения электронных музыкальных инструментов в музыкальное образование является обеспечение информационно-психологической безопасности образовательного процесса, включая:

- формирование осознанного использования технологий;
- сохранение необходимого творческого баланса между цифровыми технологиями и музицированием на акустических инструментах;
- соблюдать технику безопасности при работе с синтезатором (правильно пользоваться электронной аппаратурой и регулировать громкость звука);
- обеспечение психолого-педагогического сопровождения творческого и образовательного процесса;
- создание комфортных условий для каждого обучающегося;
- создание условий для раскрытия его индивидуальности и развития творческих способностей.

Заключение. Клавишный синтезатор, изменяя традиционные методы преподавания, позволяет сделать содержание музыкального образования более высокотехнологичным и интенсивным, помогает обогатить и расширить исполнительскую творческую деятельность, обеспечивая интеграцию традиционных педагогических подходов с современными цифровыми технологиями.

#### СПИСОК ЛИТЕРАТУРЫ

1. Gorbunova I.B., Davletova K.B. Information educational environment as a resource for advancing a teacher-musician's skills in the additional children education system. Revista Conrado. 2020. V. 16. No. 74. 38-44.
2. Белов Г.Г., Горбунова И.Б. Электроника в музыкальном искусстве: влечение времени // Мир науки, культуры, образования. 2020. № 5 (84). С. 207-210.
3. Горбунова И.Б. Компьютерная студия звукозаписи как инструмент музыкального творчества и феномен музыкальной культуры // Общество: философия, история, культура, 2017. № 2. С. 87-92.
4. Горбунова, И.Б. Информационные технологии в музыке / И.Б. Горбунова // Т. 1: Архитектура музыкального звука: учебное пособие СПб.: Изд-во РГПУ им. А. И. Герцена, 2009. 175 с.
5. Горбунова, И.Б. Информационные технологии в музыке / И.Б. Горбунова // Т. 2: Музыкальные синтезаторы: учебное пособие. СПб.: Изд-во РГПУ им. А.И. Герцена, 2010. 205 с.
6. Горбунова И.Б. Музыкально-компьютерные технологии как новая обучающая и творческая среда // Современное музыкальное образование-2002. Материалы Международной научно-практической конференции. Российский государственный педагогический университет им. А.И. Герцена, Санкт-Петербургская государственная консерватория им. Н.А. Римского-Корсакова / под общ. ред. И.Б. Горбуновой. СПб., 2002. С. 161-169.
7. Горбунова, И.Б., Давлетова, К.Б. Информационная компетентность педагога-музыканта системы дополнительного образования детей / И.Б. Горбунова, К.Б. Давлетова // Теория и практика общественного развития, 2015. № 21. С. 254-258.
8. И.Б. Горбунова, К.Б. Давлетова, С.В. Мезенцева. Музыкальные инструменты цифровой эпохи: монография /. СПб.: РГПУ им. А.И. Герцена, 2021. 188 с.
9. Горбунова, И.Б., Давлетова, К.Б. Электронные музыкальные инструменты в системе общего музыкального образования / И.Б. Горбунова, К.Б. Давлетова // Теория и практика общественного развития, 2015. № 12. С. 411-415.
10. Горский, В.А., Журкина, А.Я. Педагогические принципы развития системы дополнительного образования / В.А. Горский, А.Я. Журкина // Дополнительное образование, 1999. №2. С.4-6.
11. Давлетова К.Б. Информационная образовательная среда курсов повышения квалификации педагога-музыканта (секция «Электронные музыкальные инструменты») // Мир науки, культуры, образования. 2021. № 3 (88). С. 335-338.
12. Давлетова, К.Б. Особенности профессиональной деятельности педагога-музыканта системы дополнительного образования детей. Мир науки, культуры, образования. Международный научный журнал. Декабрь, 2016 г, №6 (61).
13. Красильников, И.М. Музыкальное искусство и образование XXI века / И.М. Красильников // Сборник материалов международной научно-практической конференции «Современное музыкальное образование 2010». СПб.: Изд-во «Лема», 2011. С. 22-28.
14. Красильников, И.М. Педагогика цифровых искусств новое направление развития теории и практики художественного образования / И.М. Красильников // Проблемы современного образования. 2011. № 6. С. 11-123.
15. Красильникова, В.А. Использование информационных и коммуникационных технологий в образовании: учебное пособие / В.А. Красильникова. Оренбург: ОГУ, 2012. 291 с.

УДК 070.1; 304.4

#### СОЦИОКУЛЬТУРНЫЕ ЦЕННОСТИ ВОЕННОЙ ЖУРНАЛИСТИКИ КАК АКСИОЛОГИЧЕСКИЙ ИНСТРУМЕНТ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Ерофеева Ирина Викторовна<sup>1</sup>, Михалева Людмила Игоревна<sup>2</sup>

<sup>1</sup> Забайкальский государственный университет

Александровская, 30, Чита, 672039, Россия

<sup>2</sup> Волгоградский государственный университет

Университетский пр., 100, Волгоград, 400062, Россия

e-mails: irina-jour@yandex.ru, mihaleva2004@mail.ru

**Аннотация.** Представлены результаты лингвокультурологического анализа медиадискурса военных журналистов, выделены доминирующие социокультурные ценности, которые являются не только когнитивными конструктами обработки фактуры языковой личностью автора, но и способны поддерживать состояние защищенности национальных интересов России.

**Ключевые слова:** военная журналистика; национальная безопасность; языковая личность журналиста; медиадискурс; национальная картина мира; социокультурные ценности.

## SOCIOCULTURAL VALUES OF MILITARY JOURNALISM AS AN AXIOLOGICAL INSTRUMENT OF NATIONAL SECURITY

Erofeeva Irina<sup>1</sup>, Mikhaleva Lyudmila<sup>2</sup>

<sup>1</sup>Transbaikal State University

30 Aleksandro-Zavodskaya st., Chita, 672039, Russia

<sup>2</sup>Volgograd State University

Universitetsky Ave., 100, Volgograd, 400062, Russia

e-mail: irina-jour@yandex.ru; natiyashiladze@mail.ru

**Abstract.** The article presents the results of the linguacultural analysis of the media discourse of military journalists, highlights the dominant sociocultural values, which are not only cognitive constructs of processing the texture by the linguistic personality of the author, but are also capable of maintaining the state of protection of Russia's national interests.

**Keywords:** military journalism; national security; journalist's linguistic personality; media discourse; national picture of the world; socio-cultural values.

Доминирующие информационные потоки российских массмедиа заполнены материалами о специальной военной операции, в которых присутствуют темы, крайне важные для большинства жителей страны. Поэтому сегодня работа военного журналиста связана не только с информированием и документализацией событий, умением работать в сложных и потенциально опасных условиях, но и со способностью понимать первопричину и глубину происходящего, видеть вектор развития национальной истории, обеспечивая информационную и национальную безопасность страны.

Результаты предлагаемого исследования опираются на проведённый нами лингвокультурологический анализ более 250 материалов о специальной военной операции ряда журналистов (Дмитрий Григорьев, Александр Коц, Дмитрий Стешин, Дарья Асламова, Юлия Андриенко), которые были опубликованы в интернет-изданиях «Аргументы и факты», Комсомольская правда, Правда.Ру. (Pravda.RU) с 2022 по 2024 гг. В процессе работы были задействованы поисковые системы Яндекс и Гугл, специализированные рубрики военкоров и подборки «Комсомольской правды» (<https://www.kp.ru/daily/theme/16422/>) и «АиФ» (<https://perm.aif.ru/opinion/author/21326?ysclid=m1hntbq3o0398605518>).

В рамках исследования медиадискурс мы рассматриваем как пространство аккумуляции и передачи социокультурных ценностей от автора к потребителю, как формат накопления и трансляции культурных норм и ценностей российского общества [4]. Человек, будучи социальным существом, предпочитает жить в гармонии с базовыми фундаментальными ценностями, соотнесёнными со знаковыми реалиями его культуры и объединяющими основные представления людей относительно целей и норм своего существования [3, с. 3]. Как отмечает Г. П. Выжлецов, ценности позволяют увидеть культуру народа и общества изнутри, из глубин социальной и индивидуальной жизни [2]. По мнению Момджян К. Х., они демонстрируют критерии мотивационного выбора человека [7].

Медиаэксперт Л. В. Баева пишет о ценностях как о необходимых инструментах жизни личности в выражении «внутренней свободы и возможности субъективации внешнего бытия» [1, с. 8]. По мнению исследователя, ценность проявляется в трёх компонентах жизни человека: *значимость, смысл и переживание*. Ценность становится реальностью, когда она человеком ощущается, осознаётся и осмысливается интуитивно и интеллектуально.

Социокультурные ценности выступают как признанные обществом ориентиры, некие устоявшиеся общепринятые убеждения, воплощающие традиционный уклад жизни. Они формируются вековым развитием народа, несут в себе коллективную память поколений и воспроизводятся в процессе социализации и в повседневной жизни, передаются от поколения к поколению, определяя основы общественного жизнеустройства [7]. Эти ценности имеют объединяющий характер, связывая культурные устои прошлого с реалиями современности. Утрата национальных ориентиров ведет к деградации культурной идентичности, превращению нации в безликое общество, лишенное корней, традиций и исторических воспоминаний, — крайне уязвимое в условиях современной глобальной информационно-психологической войны. Сохранение и тиражирование в массмедиа базовых фундаментальных ценностей социума способствует национальной безопасности — состоянию защищенности национальных интересов, а также сохранению единства в приверженности жителей страны к исконной культуре и общепринятым ценностным нормам, и традициям.

Согласно данным современной когнитивной лингвистики, языковая личность автора является носителем национальной картины мира или упорядоченной системы представлений о мире и окружающей действительности типичного представителя социума, которая отличается самобытностью и национально-культурным своеобразием [5]. В данном контексте языковая личность журналиста имманентно воспроизводит в медиадискурсе ценности социума и своей культуры, воспринимая и интерпретируя реальность концептуальными ресурсами родного языка. Осуществлённый анализ медиадискурса военных журналистов разных интернет-изданий показал гармоничное слияние индивидуальных характеристик журналиста и конструкторов национального мировидения. Духовные модели восприятия действительности особо становятся востребованными в эпоху войны, как проявление терминальной аргументации на грани ключевых ценностных категорий: жизнь-смерть,

бытие-небытие, благополучие-катастрофа. Осознание смерти даёт всем и всему подлинную ценность, укореняет в незыблемом и вечном [6].

Согласно результатам исследования, в дискурсе военных журналистов преобладают ядерные конструкты ценностного мировидения: *вера в победу, взаимовыручка, искренность, милосердие, любовь к родине, жизни и другим людям, самоотверженность* [4].

Анализируя содержание статей журналистов, как мужчин, так и женщин, можно выделить ключевые ценностные приоритеты: *ответственность, самопожертвование, патриотизм, жизнелюбие*. Частотно встречается также мотив *веры в справедливость и неизбежность возмездия врагам*, особенно выраженный в дискурсе мужчин. Ценности *взаимопомощи* сильнее проявляются в женских материалах.

Сознательно и архетипически журналисты конструируют своеобразные прототексты, основанные на исторической памяти и канонически поддерживающие должные образцы поведения человека, закреплённые в культурном коде страны. Осознание текущих событий через призму духовного и нравственного восприятия позволяют оценить происходящее в пространственно-временной перспективе с учётом исторического наследия своего народа и возможного будущего. Это помогает создавать материалы о судьбах конкретных людей, наполненные надеждой на лучшее и верой в торжество неминуемой справедливости. Сегодня профессиональная объективность журналиста заключается не в поверхностном отражении действительности, а в глубоком понимании основной сути явлений, которую журналист осознаёт, чувствует, принимает близко к сердцу и убедительно передаёт своей аудитории с учётом общих для создателя и потребителя контента национальных ценностей.

#### СПИСОК ЛИТЕРАТУРЫ

1. Баева Л. В. Экзистенциальная природа ценностей: автореферат дис. ... доктора философских наук: 09.00.13. Волгоград, 2004. 43 с.
2. Выжлецов Г. П. Аксиология культуры. СПб.: СПбГУ, 1996. 152 с.
3. Динамика ценностей населения реформируемой России. М.: Эдиториал УРСС, 1996. 224 с.
4. Ерофеева И. В., Михалева Л. В. Аксиологический потенциал эмоционального интеллекта военного журналиста в медиадискурсе // Гуманитарный вектор. 2024. Т. 19, № 4. С. 132–140. doi: 10.21209/1996-7853-2024-19-4-132-140.
5. Карасик В. И. Языковой круг: личность, концепты, дискурс. Волгоград: Перемена, 2002. 477 с.
6. Митрополит Сурожский Антоний. Труды. М.: «Практика», 2002. 1080 с.
7. Момджян К.Х. О проблеме общечеловеческих ценностей // Вопросы философии. 2020. № 3. С. 25–41.
8. Mchedlova E.M. The Impact of the Crisis on the Development of Socio-cultural Processes and Values // Вестник Национальной академии наук Республики Казахстан. 2021. Т. 5. № 393. С. 199–204.

УДК 101.3; 004.81

#### КОГНИТИВНЫЕ ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИИ

Кефели Игорь Федорович<sup>1</sup>, Кефели Константин Игоревич<sup>2</sup>

<sup>1</sup> Северо-Западный институт управления - филиал РАНХиГС  
Средний пр. В.О. 57/43, Санкт-Петербург, 199178, Россия

<sup>2</sup>Российская Ассоциация международного права  
Знаменка ул., 10, Москва, 119019  
e-mails: geokefeli@mail.ru, kefeli.kostik@mail.ru

**Аннотация.** Когнитивные технологии определяются как практические нейробиологические технологии, социальные практики, методы формирования мировоззрения и научной идеологии.

**Ключевые слова:** когнитология; когнитивная война; когнитивная безопасность; когнитивные технологии; национальная безопасность России.

#### COGNITIVE TECHNOLOGIES FOR ENSURING NATIONAL SECURITY OF RUSSIA

Kefeli Igor <sup>1</sup>, Kefeli Konstantin <sup>2</sup>

Russian Presidential Academy of National Economy and Public Administration  
57/43 Sredny Av. VI., St. Petersburg, 199178, Russia

Russian Association of International Law  
10 Znamenka St, Moscow, 119019, Russia  
e-mails: geokefeli@mail.ru, kefeli.kostik@mail.ru

**Abstract.** Cognitive technologies are defined as practical neurobiological technologies, social practices, methods of forming worldviews and scientific ideology.

**Keywords:** cognitive science; cognitive warfare; cognitive security; cognitive technologies; Russian national security.

Решение задач обеспечения национальной безопасности, включающей безопасность государства и личности, различных видов общественной безопасности (в т.ч. и информационной) основано на утверждении приоритета предупредительных мер и организации масштабной научной и образовательной деятельности в области обеспечения национальной безопасности современной России как глобальной проблемы. Вспомним интригующее заявление Генерального секретаря ООН А. Гутерриша в обращении к Генеральной Ассамблее в

январе 2020 г.: «Я представляю „четыре всадников“ — четыре надвигающиеся угрозы, которые препятствуют прогрессу и подвергают риску возможности XXI в.». И далее он назвал этих «четыре всадников», прибегнув к библейскому образу «Четырех всадников Апокалипсиса» (воплощенному Альбрехтом Дюрером в серии гравюр в канун предсказанного церковными служителями конца света на 1500 г.): геополитическая напряженность, климатический кризис, глобальное недоверие и технологические недостатки («темная сторона цифрового мира»), которые «могут поставить под угрозу наше общее будущее... Мы должны решить эти четыре проблемы XXI в.» [1]. Все более в массовом сознании утверждается признание того, что мы живем в «эпоху отсутствия безопасности», олицетворяющую совокупность экологических, геополитических, экономических, социальных и технологических рисков. Причем сам по себе глобальный риск определяется как некое «неопределенное событие или условие, которое, в случае его возникновения, может оказать значительное негативное воздействие на несколько стран или отраслей в течение последующих 10 лет» [2]. В «Докладе о глобальных рисках 2024» это «неопределенное событие» наконец-то обрело свое название — *дезинформация, созданная искусственным интеллектом*. Но самое печальное — согласно прогнозу, дезинформация в ближайшие два года ожидается как самый серьезный глобальный риск: «как иностранные, так и внутренние субъекты будут использовать дезинформацию для дальнейшего расширения социальных и политических разногласий» [3]. Такая же резкая оценка дезинформации как угрозы информационному пространству была зафиксирована и в докладе 2025 г.: «распространение ложной информации усиливает социальную поляризацию, подрывает доверие к институтам и создает благоприятные условия для манипуляций общественным мнением, становится катализатором нестабильности, особенно в условиях усиления геополитических и экономических разногласий» [4].

Столь утвердительное заявление экспертов заставляет задуматься о том, что эпицентр глобальных рисков все более активно перемещается в медиaprостранство, ментальную, когнитивную сферу человеческого бытия, которые формируют предметное поле когнитологии. Вполне серьезно один наш знакомый профессор заявил, что он начинает опасаться писать свои новые философские статьи, поскольку стоит только нажать на какую-то клавишу компьютера, как тут же ИИ выдает ему готовый текст статьи на основе заранее составленных аннотации и ключевых слов. Как-то невесело и даже жутковато становится...

Все более актуальной становится проблема разработки системы когнитивных технологий как одного из ключевых звеньев НБИКС-технологий, определяющих ядро критических технологий и нового технологического уклада в целом [5]. Это вполне объяснимо, поскольку один из вариантов когнитивной биотехнологии, относящейся к нейробиологии, позволяет «заглядывать» в сознание человека. Совокупность больших данных, открытых источников, социальных сетей, массового наблюдения, технологий распознавания лиц, геолокации и искусственного интеллекта при использовании когнитивных технологий позволяет обеспечивать доступ к мозгу лиц, принимающих решения, что в 2019 г. в программе НАТО «Операция 2040» было определено как *the centre of gravity*. Более поздние исследования предоставили подробное и научное понимание того, почему когнитивная сфера находится под постоянной угрозой [6]. Основные западные разработчики когнитивной войны в своей деятельности вовлекают не только военный потенциал, но и призывают трансформировать гражданские научные знания в военные с активным участием крупных транснациональных корпораций. В условиях деструктивного когнитивного воздействия военно-политическому руководству Российской Федерации требуется выработать и реализовать ряд превентивных мер по нейтрализации вредоносного влияния информационных и психоэмоциональных технологий когнитивной войны, создать базовые условия в государстве для осуществления кардинальных решений по ряду направлений:

- создание в образовательной сфере условий для становления и укрепления мировоззрения молодого поколения;

- организация планомерной разъяснительной работы о методах, целях и способах когнитивной войны. Это позволит консолидировать и сплотить российское общество для противодействия враждебным замыслам и действиям коллективного Запада. Сплоченность является следствием и показателем укрепления доверия граждан к институтам власти, достижения долгосрочной стабильности и общественного согласия;

- совершенствование государственной политики по повышению качества жизни граждан за счет создания современной и доступной системы образования, выработка комплексных мер, направленных на преодоление негативных демографических тенденций и решение системных проблем в области здравоохранения, снижение уровня бедности и расслоения общества по уровню доходов;

- создание кардинально новых правовых оснований и реальных механизмов, с помощью которых институты гражданского общества могли бы контролировать деятельность бизнеса и органов государственной власти (например, создание государственного фонда поддержки участников специальной военной операции «Защитники Отечества»), а также влиять на распределение национальных ресурсов;

- разработка и внедрение комплексной программы работы с населением по информационному и психологическому образованию, разъяснению деструктивной составляющей, распространяемой государствами коллективного Запада информации.

Таким образом, сегодня необходимо активизировать, подкрепленную научными исследованиями практическую деятельность федеральных и региональных органов государственной власти по защите от «внешнего деструктивного информационно-психологического воздействия» и «формированию безопасного информационного пространства, защите российского общества от распространения деструктивной идеологии», как это предусмотрено в «Основах государственной политики по сохранению и укреплению традиционных

российских духовно-нравственных ценностей (Утверждены Указом Президента Российской Федерации от 9 ноября 2022 г. № 809). Более того, не меньшую актуальность занимают вопросы подготовки научных кадров, технологов по широкому спектру когнитивных исследований, разработок и социальных практик.

#### СПИСОК ЛИТЕРАТУРЫ

1. Guterres A. Remarks to the General Assembly on the Secretary-General's priorities for 2020 // Официальный сайт ООН. 22.01.2020 [Электронный ресурс]. URL: <https://www.un.org/sg/en/content/sg/speeches/2020-01-22/remarks-general-assembly-priorities-for-2020> (дата обращения: 12.08.2025).
2. The Global Risks Report 2019, 14th Edition, is published by the World Economic Forum. Geneva, 2019. 108 p. P. 96-97.
3. WEF The Global Risks Report 2024 (Chapter 1.3: Misinformation [https://www3.weforum.org/docs/WEF\\_The\\_Global\\_Risks\\_Report\\_2024.pdf](https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf)).
4. WEF The Global Risks. Report 2025. 20th Edition. Insight Report, p. 9.
5. Васильев Ю.С., Кефели И.Ф., Колбанев М.О. Роль критических технологий в обеспечении глобальной безопасности // Известия Российской Академии Ракетных и Артиллерийских Наук. Вып. (107). 2019. С. 34-41.
6. NATO 2022 Strategic Concept. Adopted by Heads of State and Government at the NATO Summit in Madrid 29 June 2022 P. 3-4. URL: [https://www.nato.int/nato\\_static\\_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept](https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept). (дата обращения 11.08.2025).

УДК 101.1; 159.9

#### РЕЧЕВОЕ ПОВЕДЕНИЕ КАНЦЛЕРА ГЕРМАНИИ: ПРЕДПОЧТЕНИЕ — МЕНАСИВАМ

Мисонжников Борис Яковлевич

Санкт-Петербургский государственный университет  
Университетская наб., 7–9, г. Санкт-Петербург, 199034, Россия  
e-mail: b.misonzhnikov@spbu.ru

**Аннотация.** Рассматриваются аспекты речевого поведения канцлера Германии Фридриха Мерца, его публичные высказывания, в которых содержится прямая угроза руководству Российской Федерации. Политические менасивы канцлера дестабилизируют международную обстановку, пагубно влияют на межнациональные отношения. Отмечается, что заявления Мерца, занимающего высокое положение в иерархии западных политиков, крайне опасны тем, что обретают перформативный эффект, становятся крайне деструктивными в отношении информационно-психологической безопасности общества.

**Ключевые слова:** канцлер Германии; речевое поведение; менасив; информационно-психологическая безопасность; перформативный эффект.

#### SPEECH BEHAVIOR OF THE GERMAN CHANCELLOR: PREFERENCE FOR MENASIVAS

Misonzhnikov Boris

Saint Petersburg State University  
7–9 Universitetskaya Naberezhnaya, Saint Petersburg, 199034, Russia  
e-mail: b.misonzhnikov@spbu.ru

**Abstract.** The article examines the aspects of the speech behavior of German Chancellor Friedrich Merz, as well as his public statements that contain direct threats to the leadership of the Russian Federation. The Chancellor's political statements have destabilized the international situation and had a detrimental impact on interethnic relations. It is noted that Merz's statements, as a high-ranking Western politician, are extremely dangerous because they have a performative effect and become highly destructive in terms of the information and psychological security of society.

**Keywords:** German Chancellor; speech behavior; menasiv; information and psychological security; performative effect.

Фридрих Мерц, лидер консервативного блока Христианско-демократического союза и Христианско-социального союза (ХДС/ХСС) стал федеральным канцлером Германии в мае 2025 г., причем первый раунд голосования для него закончился неудачей: впервые в истории ФРГ кандидат на пост канцлера лишь со второй попытки — да и то в итоге хитроумных коалиционных переговоров — смог получить поддержку членов бундестага. У нового главы федерального правительства примечательное происхождение: отец воевал на Восточном фронте в составе вермахта, а дед по материнской линии еще в 1933 г. вступил в нацистскую партию (НСДАП) и в звании обершарфюрера служил в СА — штурмовом отряде, представляющем собой боевую организацию партии. То есть Мерц вырос в окружении людей, как можно предположить с полным на то основанием, преданным нацистской идеологии. Едва став канцлером, он проявил себя как радикальный сторонник реваншизма и убежденный приверженец применения военной силы в экспансионистских целях.

И еще один немаловажный факт: Мерц по материнской линии — потомок древнего рода Совиньи, детство провел в родовом особняке и, повзрослев, пошел по пути многих европейских аристократов. Партийную работу в консервативном блоке совмещал с занятием руководящих должностей в нескольких банках, страховых компаниях, в управлении крупного химического концерна и, что самое важное, в немецком подразделении американской инвестиционной компании BlackRock. Там он был председателем наблюдательного совета. Между прочим, это самая крупная в мире компания по размеру активов под управлением, т.е. под этим подразумевается общая рыночная стоимость всех инвестиций, которыми управляет компания от имени клиентов. Размер этих активов под управлением в компании BlackRock за апрель — июнь 2025 г. составил около 12,5 трлн долларов! Правда, Мерц компанию уже покинул, чтобы не создавать «конфликта интересов». Так что Мерц — отнюдь не бедный аристократ, что необходимо учитывать при рассмотрении мотивов его поступков. Они обусловлены не только



пронацистским воспитанием, но и классовыми, имущественными факторами, ради соответствия которым канцлер, несмотря на крайне правое и шовинистическое мировоззрение, надевает кипу и выступает в синагоге.

Всей совокупностью причин — как идейных, так и материальных — обусловлено поведение Мерца, включая и речевое. Пожалуй, ни один канцлер всего послевоенного периода не позволял себе демонстрировать такого пренебрежительного, оскорбительного и неприязненного отношения к России и ее первым лицам, как это позволяет себе Мерц. По-видимому, его доминирующие поведенческие паттерны обусловлены, во-первых, трансгенерационными духовно-идеологическими причинами, включая даже национально-травматические, сочетающиеся с желаниями отмщения, а во-вторых, причинами сугубо прагматическими, совершенно меркантильными. То есть агрессивная риторика канцлера представляет собой сочетание эмотивного и несдержанного, по сути своей зачастую непристойного фразёрства и продуманных, подстрекательских заявлений, формирующих поле провокативного дискурса. Т.А. Воронцова отмечает: «Психологическая наука трактует вербальную агрессию как проявление негативных эмоций по отношению к чему-либо или к кому-либо, выраженное в речи. Однако с позиций коммуникативной лингвистики важно не только как сказано, но и для чего сказано» [1]. Как опытный политик, Мерц, вне всякого сомнения, хорошо представляет себе последствия проявленной им речевой агрессии. Т.А. Воронцова далее подчеркивает: «Мы рассматриваем речевую агрессию как целенаправленное, мотивированное, преимущественно контролируемое (через сознательный выбор речевых стратегий и тактик, а также отбор речевых и языковых средств) речевое поведение. <...> С точки зрения диалогического взаимодействия, речевая агрессия — это установка адресанта на антидиалог в широком смысле слова» [1]. Мерц, таким образом, своим поведением практически делает невозможным диалог с российской стороной.

По отношению к России и ее политическому руководству едва ли не во всех выступлениях Мерца красной нитью проходят угрозы, которые можно идентифицировать как имплицитные и эксплицитные. По утверждению Е.Ю. Сидоровой, «если агрессия в речи представлена имплицитно (косвенно, замаскировано), мы говорим о косвенных вербально-агрессивных актах» [2]. И в выступлениях Мерца — особенно до того, как он прошел процедуру избрания на пост канцлера — превалировала именно имплицитная речевая агрессия, которая проявлялась не только вербально, а именно в не столь резких политических заявлениях, но и в паралингвистическом аспекте — например, политик позволял себе негативно-ироничный тон в отношении России и ее лидеров. Для манифестаций открытого менасивного поведения у Мерца было меньше возможностей. Но после избрания канцлером он стал допускать заявления явно русофобского и очень резкого характера. А.А. Романов и О.В. Новоселова справедливо обращают внимание на то, что до завершения выборов «политики избегают частого использования таких форм высказываний-угроз, чтобы не запугать избирателей возможными менасивными последствиями» [3]. Нынешний канцлер, конечно, не был исключением.

Заявления Мерца, который занял высокую должность, обретают несравненно более значительный вес, поскольку теперь он выступает в качестве лидера Германии. В его риторике, тем не менее, остается некая иррациональность и фантазийность, по-прежнему присутствует эмотивно-идеологическая составляющая. Так, он утверждал в интервью, что «Владимир Путин хочет восстановить Советский Союз», на что последовала жесткая реакция известного журналиста Томаса Рёпера, назвавшего Мерца «лгуном», так как Путин ничего подобного говорить не мог [4]. Однако в современных высказываниях канцлера, отражающих его политическую позицию, в большей мере ощущается именно конкретно-прагматический подход, который обусловлен отнюдь не трансгенерационными факторами, существующими не без доли сентиментальности, а сугубо корыстными мотивами и холодным расчетом. Канцлер инициирует получение суммы почти в триллион евро на армию и инфраструктуру Германии, и можно не сомневаться в том, что резкое повышение расходов на вооруженные силы будет приоритетом в немецкой политике. Потенциальный противник — Россия, с которой, по словам канцлера, существуют конфликтные отношения. История с деньгами не совсем ясная: Германии придется платить из бюджета страны оружием компаниям, многие из которых принадлежат иностранцам. Транснациональным корпорациям нужна война, и Мерц выступает яростным сторонником этой аферы. К слову сказать, немецкий концерн Rheinmetall AG, один из крупнейших производителей военной техники и вооружения, строит заводы в Румынии, Венгрии и Литве, перестраивает завод Volkswagen с целью производства вооружений. Даже по самым скромным подсчетам доходы Rheinmetall AG в 2025 г. вырастут на 30 %.

Реализации этих планов нужно идеологическое обеспечение, и в данном случае наиболее подходящая форма — вербальная. В контексте событий высказывания канцлера обретают перформативный эффект, слова становятся действием. Но происходит глубинный онтологический сбой: дискурс, который призвано формировать лицо, наделенное очень большой — практически исключительной — властью, деконструируется, утрачивает очертания в силу того, что субъект речемыслительной практики теряет социальные ориентиры. Дискурс не может формироваться и существовать в пространстве, в котором идут процессы симулякризации, и, как отмечает В.И. Демченко, «симулякр начинается там, где заканчивается подобие» [5]. В этом искаженном социально-политическом пространстве не может адекватно осуществляться перформативная функция. Иллокутивная цель вещающего субъекта будет совершенно не такой, какой предполагается. Возникает, по сути, метафизически тупиковая ситуация. Вероятно, ее имела в виду Л.А. Романова, отмечая, что «с трудом определяется ситуация, когда используется перформатив в его каноническом употреблении, а когда функционирует перформанс как исполнение, отвечающее лишь определенным (отдельным) условиям перформативных речевых актов» [6].

Речевое поведение Фридриха Мерца отличается высоким уровнем вербальной агрессии, отсутствием реальных аргументов, что ведет к искажению дискурсного пространства, не способствует формированию реальной

картины мира. Анализ политической ситуации в его заявлениях подменяется поверхностными, часто не соответствующими действительности пропагандистскими клише, выступления изобилуют политическими менасивными декларациями, формируют негативный образ России и демонизируют ее народ. Это разрушает основания для нормальных отношений, не способствует взаимопониманию и оздоровлению международного климата. Преднамеренная, осуществляемая в корыстных интересах симулякризация политического и социокультурного пространства может иметь совершенно определенный негативный результат, вызвать процесс дегуманизации социума.

#### СПИСОК ЛИТЕРАТУРЫ

1. Воронцова Т.А. Речевая агрессия: коммуникативно-дискурсивный подход: автореф. дис. ... д-ра филол. наук. Челябинск, 2006. 44 с.
2. Сидорова Е.Ю. Вербальная агрессия как коммуникативно-прагматическое явление // Вестн. Том. гос. ун-та. 2009. № 319. С.28–31.
3. Романов А.А., Новоселова О.В. Предвыборные менасивы как особый прагматический тип высказываний со значением угрозы // Вестн. Сев. (Арктич.) федер. ун-та. Сер.: Гуманит. и соц. науки. 2020. № 1. С. 44–52.
4. Röper Th. Wenn Friedrich Merz über Russland spricht... // Anti-Spiegel. 2025. 2. Sept.
5. Демченко В.И. Симулякризация социокультурного пространства // Вестн. Ставропольск. гос. ун-та. 2009. № 61. С. 106–110.
6. Романова Л.А. Композитные перформативы в функциональной парадигме языка: семантический и прагматический аспекты: автореф. дис. ... д-ра филол. наук. Великий Новгород, 2010. 48 с.

УДК 304.5

#### КОГНИТИВНЫЕ МЕХАНИЗМЫ СОЦИАЛЬНЫХ СИСТЕМ

Плебанек Ольга Васильевна

Санкт-Петербургский государственный университет  
Университетская наб., 7–9, Санкт-Петербург, Россия, 199034  
e-mail: plebanek@mail.ru

**Аннотация.** Предлагается рассмотрение общества как когнитивной системы, в которой безопасность и выживаемость общественных систем находится в зависимости от механизмов, обеспечивающих производство и циркуляцию информации

**Ключевые слова:** автопоэзис; когнитивная система; концепция биокультурной эволюции; когнитивные механизмы; социальные институты; гибридная война; надрациональные драйверы поведения.

#### COGNITIVE MECHANISMS OF SOCIAL SYSTEMS

Plebanek Olga

St. Petersburg State University  
7-9 Universitetskaya Embankment, Saint Petersburg, Russia, 199034  
e-mail: plebanek@mail.ru

**Abstract.** It is proposed to consider society as a cognitive system in which the safety and survival of social systems depend on the mechanisms that ensure the production and circulation of information.

**Keywords:** autopoiesis; cognitive system, the concept of biocultural evolution; cognitive mechanisms; social institutions; hybrid warfare; supranational drivers of behavior.

Классические концепции общественной безопасности базировались на парадигмах, выработанных в классической и неклассической науке, поэтому оказались неэффективными в эпоху гибридных войн. Безопасность государства не достигается наращиванием традиционных мощностей и не сводится к эффективным техническим, технологическим и организационным средствам. Концепция безопасности, в основе которой лежит модель информационной войны, также является ограниченной по своим возможностям, так как полем активных действий информационной войны являются информационные системы. Несмотря на то, что основным объектом информационных деструктивных воздействий является индивидуальное и общественное сознание, противодействие информационным атакам конструируется, главным образом, как технико-технологическое. Современная концепция безопасности в условиях гибридных войн должна опираться на системный подход и не сводится к контролю информационных потоков.

Современные научные концепции позволяют связать воедино арсенал естественных, социальных, гуманитарных и технических наук для создания стратегии безопасности в условиях когнитивных войн, целью воздействия которых является целостная общественная система и надрациональные драйверы поведения. Постнеклассическая парадигма предлагает модель мироздания, в которой все динамичные системы, способные к сохранению жизнеспособности в изменяющейся реальности, являются саморазвивающимися, а поэтому способны создавать новые уровни организации и новые подсистемы из имеющихся ресурсов для сохранения траектории развития. В этой парадигме в 70-е гг. XX в. чилийскими нейрофизиологами У. Матураной и Ф. Варелой была предложена концепция эвтопоэзиса, в основе которой лежит когнитивная модель жизни: «живые системы — это когнитивные системы, а жизнь как процесс — это процесс познания. Это утверждение справедливо для всех организмов, с нервной системой или без нее» [1]. Примерно в это же время, Р. Бойд и П. Ричерсон предложили концепцию биокультурной эволюции [2], которая включала разум и культуру в единую эволюционную теорию. Концепцию генно-культурной эволюции стали развивать Ч. Ласмдэн и Э. Уилсон, в работах которых была вскрыта

более широкая связь не только естественных и общественных наук, но связь между порядком и сложностью биологических и культурных систем и некоторыми основополагающими законами [3, с. 92].

Один из соавторов концепции автопознания, У. Матурана, позднее распространил идею на общественные процессы и высказал мысль, что социальные системы могут быть поняты как когнитивные системы. С нашей точки зрения, тезис Матураны и Варелы «жить означает познавать (жить означает совершать эффективные действия в области существования в качестве живых существ)» [1, с. 154] закономерно распространяется на функционирование социальных систем, так как эффективность существования и выживаемость обществ напрямую зависят от способности общества отвечать на Вызовы среды и давать адекватные Ответы (концепты введенные А. Тойнби для объяснения культурной динамики и многообразия культурных систем [4] в виде конкретных социальных институтов. От того, насколько эффективны эти социальные институты будут в процессе решения проблем, стоящих перед обществом, зависит конкурентоспособность этих социальных систем. Очевидно, что решение стоящих перед обществом проблем распадается на ряд когнитивных задач: обнаружение проблем, извлечение необходимых данных из предшествующего опыта, символизация этого знания и трансляция паттернов и т.д. Таким образом, чем более сложные проблемы стоят перед общественной системой, чем более комплексный характер имеют вызовы, тем более системным должен быть конструируемый ответ в виде секьюритарных стратегий.

Общая теория систем, начало которой было положено Л. Фон Берталанфи, предполагает структурно-уровневую организацию любой сложной системы [5]. Функционирование такой системы подчиняется принципам вертикальной регуляции, согласно которой «исходные, более общие законы нижних уровней сохраняются на верхних уровнях с определенными ограничениями <...>, а верхние уровни в структурной организации влияют на ее нижние уровни» [6]. Принцип вертикальной регуляции и обратных связей был также обоснован в теории кибернетики как важнейший принцип управления [7]. Относительно решения нашей проблемы — построения концепции когнитивной безопасности социальных систем, в основу следует положить модель когнитивных механизмов психики, которые включают: 1) восприятие и внимание, 2) память, 3) обучение, 4) мышление и решение задач, 5) кодирование и декодирование (язык), 6) управление. При этом, в соответствии с вышеуказанным принципом вертикальной регуляции и обратной связи, социальные дериваты когнитивных механизмов психики — соответствующие социальные институты, являются драйверами поведения человека. Эти культурные драйверы имеют более значимое воздействие, чем рациональные детерминанты поведения, так как (в отличие от *иррационального* как противоположного *рациональному*) являются специфической человеческой характеристикой, помимо способности к анализу, имеющейся у животных, включающей более целостную и комплексную способность к созданию смыслов и стремлению руководствоваться этими смыслами, а не только данными об окружающей среде.

Дериватами когнитивных механизмов на социальном уровне являются специфические социальные институты для:

- *восприятия* информации и фиксации *внимания*, например, являются медиа и общественные движения, которые обнаруживают критические места в функционировании социальной системы и сигнализируют о возможных кризисах; и чем эффективнее работа этих институтов, тем своевременнее адекватная реакция соответствующих подсистем общества;

- механизм *памяти*, например, имеет развитие, помимо музеефикации и других средств исторической памяти, в появившейся культурной практике реконструкторов, индустриализации этнических культур и т.д.; эти новые формы мемориальной культуры имеют больший потенциал смыслопроизводства, чем традиционное историческое просвещение;

- *обучение* как когнитивный социальный институт, транслирующий конструируемые поведенческие паттерны и культурные модели, например, получил актуализацию в форме социальной рекламы, которая эффективнее внедряет в общественное сознание смыслы, чем формальные нормы и декларируемые принципы;

- механизмы *кодирования* и *декодирования* информации — язык имеет продолжение как когнитивный социальный механизм, например, в государственной геральдике, политическом бренде и т.д.; визуальные и аудиальные символы надежнее кодируют поведение людей, чем рациональные объяснения, так как воздействуют на уровне надличностных регулятивов и выполняют функцию прайминга в повседневных ситуациях.

Таким образом, в основу стратегии противодействия деструктивным воздействиям и драйверам деструктивного поведения нужно положить не технологические и нормативные конструкции, а арсенал современных подходов, включающих когнитивные основания безопасности.

#### СПИСОК ЛИТЕРАТУРЫ

1. Maturana, Humberto R. & Varela, Francisco J. (1980): Autopoiesis and Cognition. [электр. ресурс]. Режим доступа: [https://en.wikipedia.org/wiki/Humberto\\_Maturana](https://en.wikipedia.org/wiki/Humberto_Maturana) (дата обращения: 03.09.2024).
2. Boyd, R. and P. J. Richerson. 1985. Culture and the Evolutionary Process. Chicago: University of Chicago Press. 1985. 331 p. ISBN: 9780226069319 [электр. ресурс]. Режим доступа: [https://openlibrary.org/books/OL2861312M/Culture\\_and\\_the\\_evolutionary\\_process](https://openlibrary.org/books/OL2861312M/Culture_and_the_evolutionary_process)
3. Ламсен Ч. Дж., Уилсон Э. О. Прометеев огонь: Размышления о происхождении человеческого разума. Пер. с англ. / Предисл. С. Г. Пилецкого. М.: урсс: Леланд, 2017. 304 с.
4. Тойнби А.Дж. Исследование истории: В 3 т. / пер. с англ., вступ. статья и коммент. К.Я. Кожурина. СПб.: Изд-во С.-Петерб. ун-та: «Издательство Олега Абышко», 2006.
5. Берталанфи Л. Фон. Общая теория систем обзор проблем и результатов // Системные исследования. Ежегодник. М., 1969. С.30-55
6. Беломестнова Н. В. Системный подход в психологии // Вестник ОГУ, 2005. Том 1. №10. Гуманитарные науки. С.43-54
7. Винер Н. Кибернетика (управление и связь в животном и машине). М.: Радио, 1966.

УДК 101.1; 159.9

**РАЗВИТИЕ КРИТИЧЕСКОГО МЫШЛЕНИЯ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ОБЩЕСТВА****Халифаева Ольга Алексеевна**

Астраханский государственный университет им. В.Н. Татищева

Татищева, ул. 20 А, Астрахань, 414056, Россия

e-mail: olha78@yandex.ru

**Аннотация.** Одной из ключевых компетенций XXI века в системе образования является критическое мышление, которое позволяет осознанно подходить к отбору и осмыслению информации. В докладе представлена проблема развития критического мышления в условиях цифровизации образования, а также противодействия информационно-негативному воздействию и решению задач обеспечения информационно-психологической безопасности личности.

**Ключевые слова:** информационно-личностная безопасность; цифровизация общества; критическое мышление; проектная работа.

**DEVELOPING CRITICAL THINKING IN THE CONTEXT OF DIGITALIZATION OF SOCIETY****Khalifaeva Olga**

V.N. Tatishchev Astrakhan State University

Tatishchev St., 20A, Astrakhan, 414056, Russia

e-mail: olha78@yandex.ru

**Abstract.** One of the key competencies of the 21st century in the education system is critical thinking, which enables a conscious approach to selecting and interpreting information. This paper presents the problem of developing critical thinking in the context of digitalization of education, as well as countering the negative impact of information and addressing the challenges of ensuring the information and psychological security of the individual.

**Keywords:** information and personal security; digitalization of society; critical thinking; project work.

В научных исследованиях последних лет понятие «критическое мышление» все больше интерпретируется с понятием «информационно-личностная безопасность» в связи с ростом влияния медиасреды на социализацию личности [1].

Само понятие в философском ключе предлагает воспринимать как преобразование активности. А с точки зрения психологии мышление реализуется через взаимодействие в ходе проектной работы, это и способствует прохождению личности в познавательной деятельности» [2].

Российские учёные А. В. Федоров, Е. В. Мурюкина, С. И. Заир-Бек и др. считают, что «критическое мышление выступает гарантом социальной безопасности и социальной стабильности у подрастающего поколения».

Многие ученые отмечают необходимость осуществления междисциплинарного подхода в изучении критического мышления, так как данная изучаемая дефиниция связана с такими понятиями как информационно-психологическая безопасность (В. Г. Грачев, А. Н. Лунев, Н. Б. Пугачева) [3], когнитивная безопасность (И. Ф. Кефели) [4], экзистенциальная безопасность (Л. В. Баева) [5]. И данные дефиниции имеет общее составляющее, это состояние защищенности личности от деструктивного информационно-психологического воздействия, что определяет актуальность и приоритетность изучения данной проблемы в контексте цифровизации образования, отсутствие системного подхода в образовательном процессе при подготовке специалистов различной направленности, так как подготовка высококвалифицированных специалистов, способных самостоятельно мыслить, анализировать, осуществлять поиск данных, аргументировать, систематизировать, структурировать информацию являются ключевыми навыками специалиста в любой отрасли, а за частую в реальности оказывается, что ожидания как выпускников, так и работодателей не всегда оправдываются. Критическое мышление выступает стимулирующим фактором научного поиска в области направления информационно-психологической и когнитивной безопасности личности.

Анализ исследований критического мышления, проведенный учеными Н. И. Мазарчук, Е. О. Мазарчук, А. Н. Соколовым, И. В. Боязитовой, Н. В. Лебедева, Л. И. Иванкиной, выявили, что показатели уровня развития навыков критического мышления у студентов в вузе незначительна, по-прежнему проблемными точками критического мышления остаются такие показатели, как «интерпретация», «анализ», «саморегуляция», в результате чего ученые акцентируют внимание на том, что необходимо вводить в образовательный процесс комплексные дисциплины, проекты, мероприятия, которые обеспечат формирование универсальной компетенции в рамках обобщенной категории «Системное и критическое мышление. В качестве примера внедрения научных разработок по когнитивной психологии для формирования навыков критического и аналитического мышления можно привести опыт ФГБОУ ВО «Астраханского государственного университета им. В. Н. Татищева», где в учебный процесс всех направлений подготовки была введена дисциплина «Когнитивные технологии». Одной из тем освоения программы является развитие критического мышления, в которой используются навыки сократической дискуссии и диалогического рассуждения, ориентация на логичность и последовательность в обработке информации, а также оценка достоверности источников информации, аргументов и теорий, на это также обращают внимание ученые И.иФ. Кефели, который придает изучению когнитивных технологий особую значимость как основе объективного знания для противодействия манипуляциям сознанием людей.

Исходя из вышесказанного, можно определить, что развитие критического мышления у студентов в период обучения в вузе входит в ранг первоочередных задач высшего образования в условиях цифровизации.

#### СПИСОК ЛИТЕРАТУРЫ

1. Курилина Ю.В., Денег Д.В. Критическое мышление как целевой ориентир формирования информационно-личностной безопасности / Актуальные вопросы педагогической науки и образования. Сборник статей по материалам авторских исследований II Всероссийской научно-практической Всероссийской студенческой научно-практической конференции. Краснодар: Кубанский государственный университет, 2022. С. 228–237.
2. Кочерга А. В. Взаимосвязь мышления, чувств и воображения в развитии критичности человека / В. Кочерга. Автореф. дис. канд. психол. наук: 19.00.01 Ин-т психологии им. Костюка АПН Украины. 2003. С. 116.
3. Рерке В.И., Бубнова И.С., Демаков В.И. Информационно-психологическая безопасность как научно-исследовательская дефиниция // Научно-педагогическое обозрение. 2022. № 5 (45). С. 202–211.
4. Кефели И. Ф. Асфатроника: на пути к теории глобальной безопасности: монография. СПб.: ИПЦ СЗИУ РАНХиГС, 2020. 228 с.
5. Баева Л.В. Экзистенциальная безопасность в условиях техногенной культуры // Вестник Российского университета дружбы народов. Серия: Философия. 2025 Т. 29 № 2 С. 282–301. <https://doi.org/10.22363/2313-2302-2025-29-2-282-301>.



## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОЦИОКОМПЬЮТИНГЕ

### РАСПРОСТРАНЕНИЕ ФЕЙКОВОЙ ИНФОРМАЦИИ В СОЦИАЛЬНЫХ СЕТЯХ НА ОСНОВЕ РАСШИРЕННОЙ МОДЕЛИ SCWIEHR

**Борисов Сергей Валерьевич**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича  
Большевикова пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mail: sergeiborisov@ieee.org

**Аннотация.** Цель работы — повышение точности прогнозов распространения слухов путем разработки уточненного описания динамики распространения деструктивной информации в социальных сетях и выработки эффективных стратегий по её сдерживанию на основе расширенной модели распространения слухов SCWIEHR. Определены условия, при которых слухи либо затухают, либо устойчиво распространяются. Модель позволяет формализовать и тестировать различные стратегии противодействия слухам, включая алгоритмическое вмешательство и работу с «молчащей» аудиторией.

**Ключевые слова:** модель распространения информации; социальные сети; информационная безопасность общества; фейковая информация; слух; разоблачение и подавление слухов; математическая модель SCWIEHR.

### SPREADING RUMORS ON SOCIAL NETWORKS BASED ON THE EXTENDED SCWIEHR MODEL

**Borisov Sergei**

St Petersburg State University of Telecommunications named after Prof. M. A. Bonch-Bruевич  
22 Bol'shevnikov Av., build. 1, St-Petersburg, 193232, Russia  
e-mail: sergeiborisov@ieee.org

**Abstract:** The aim of this study is to improve the accuracy of rumor spread forecasts by developing a more accurate description of the dynamics of destructive information dissemination on social networks and developing effective strategies to curb it based on the expanded SCWIEHR rumor spread model. We define conditions under which rumors either fade or steadily spread. The model enables the formalization and testing of various rumor countermeasure strategies, including algorithmic intervention and targeting "silent" audiences.

**Keywords:** information dissemination model; social networks; information security of society; fake information; rumor; debunking and suppression of rumors; SCWIEHR mathematical model.

Современные исследования проводятся в области безопасности информации в социальных сетях, созданной с помощью технологий искусственного интеллекта [1]. Исследуются методы социальной инженерии [1-2], бот-активности [3]. Ряд исследований показал, что слухи распространяются быстрее и шире, чем проверенная информация, способствуя поляризации общества и формированию ошибочных убеждений [4, 5, 6]. Проводится анализ моделей распространения информации в социальных группах [7]. Цель данного исследования — адаптировать эпидемиологические модели (в частности, SIR, SEIR и их модификации) к процессам распространения дезинформации в социальных сетях, а также выявить ключевые факторы, влияющие на переходы между состояниями пользователей. Предполагается построить математические и агент-ориентированные симуляции, позволяющие оценить эффективность различных стратегий противодействия слухам — от модерации и фактчекинга до повышения медиаграмотности.

В существующую модель SEIR [8] введены дополнительные категории пользователей:

C (Commenters) — лица, активно участвующие в обсуждении слухов, не обязательно способствующие их распространению;

W (Waiters) — пользователи, занимающие выжидательную позицию, демонстрирующие нейтралитет до получения дополнительных сведений;

E (Exposers) — индивиды, обладающие достоверной информацией и способные опровергать слухи;

H (Hibernators) — лица, временно прекратившие участие в распространении слухов, но сохраняющие потенциал возврата к активной фазе.

Динамика распространения и сформулированы уравнения для модели SCWIEHR.  $S(t)$ ,  $C(t)$ ,  $W(t)$ ,  $I(t)$ ,  $E(t)$ ,  $H(t)$  и  $R(t)$  представляют собой пропорции групп, в момент времени  $t$ .

Согласно описанию параметров модели, «П — скорость притока новых пользователей» и является неотрицательной константой, принимающей значения от 0 до 1 включительно. Этот приток отражает реалии социальных платформ, где ежедневно появляются новые пользователи, способные вступить во взаимодействие

с уже циркулирующими слухами. Таким образом,  $\Pi$  моделирует естественное расширение системы и сохраняет её актуальность при длительном анализе. По критериям распространения модель можно описать следующими нелинейными дифференциальными уравнениями:

$$\begin{aligned}\frac{dS}{dt} &= \Pi - (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)S - (\alpha_1 + \alpha_3)S(I + C) \\ \frac{dC}{dt} &= \alpha_1 S(I + C) + \gamma_1 W(I + C) - (\beta_1 + \beta_2 + \beta_3)C - \beta_2 CI \\ \frac{dW}{dt} &= \alpha_2 S + \beta_1 C + \sigma_1 I - (\gamma_1 + \gamma_3)W(I + C) - \gamma_2 W \\ \frac{dI}{dt} &= \alpha_3 S(I + C) + \gamma_3 W(I + C) + \beta_2 CI - (\sigma_1 + \sigma_2 + \gamma + \theta)I \quad (1.1) \\ \frac{dE}{dt} &= \gamma IE - \mu E \\ \frac{dH}{dt} &= \theta IE - (\eta + \mu)H \\ \frac{dR}{dt} &= \alpha_4 S + \beta_3 C + \gamma_2 W + \sigma_2 I + \eta H - \mu R\end{aligned}$$

Начальные условия динамической системы (1.1) удовлетворяют следующему уравнению (1.2).

$$S(0) \geq 0, C(0) \geq 0, W(0) \geq 0, I(0) \geq 0, E(0) \geq 0, H(0) \geq 0, R(0) \geq 0 \quad (1.2)$$

В рамках настоящего исследования была разработана расширенная математическая модель SCWIEHR, описывающая процесс распространения слухов в социальных сетях с учётом роли нейтральных пользователей, комментаторов, разоблачителей и временно неактивных агентов. Модель учитывает множественные траектории переходов между состояниями пользователей, а также повторяющееся «выжидательное» поведение, что делает её более реалистичной по сравнению с классическими эпидемиологическими аналогами.

#### СПИСОК ЛИТЕРАТУРЫ

1. Борисов, С. В. Актуальность проблемы выявления сгенерированного видео с использованием технологий искусственного интеллекта в социальных сетях и цифровых медиа / С. В. Борисов // Безопасные информационные технологии : Сборник трудов Тринадцатой международной научно-технической конференции, Москва, 30 октября – 01 ноября 2024 года. – Москва: МГТУ им. Н.Э.Баумана, 2024. – С. 42-45. – EDN IMJYMW.
2. Борисов, С. В. Определение признаков фишинговых сообщений в электронной почте / С. В. Борисов, В. А. Севостьянов, А. Ю. Цветков // Студенческая весна - 2023 : Материалы 77-ой региональной научно-технической конференции студентов, аспирантов и молодых ученых, Санкт-Петербург, 23–24 мая 2023 года. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2023. – С. 88-92. – EDN OEBILD.
3. Борисов, С. В. Боты в социальных сетях / С. В. Борисов, А. А. Мосиян, Д. В. Сахаров // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2024) : Сборник научных статей XIII Международной научно-технической и научно-методической конференции, Санкт-Петербург, 27–28 февраля 2024 года. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2024. – С. 560-563. – EDN YBALCT.
4. Allcott H., Gentzkow M. Social Media and Fake News in the 2016 Election // Journal of Economic Perspectives. 2017. Vol. 31, No. 2. P. 211–236.
5. Lazer D.M. J. et al. The science of fake news // Science. 2018. Vol. 359(6380). P. 1094–1096.
6. Vosoughi S., Roy D., Aral S. The spread of true and false news online // Science. 2018. Vol. 359(6380). P. 1146–1151.
7. Сахаров, Д. В. Анализ моделей распространения информации в социальных группах / Д. В. Сахаров, С. В. Борисов // 65-я научно-техническая конференция профессорско-преподавательского состава, научных работников и аспирантов (НТК ППС 2025) : Сборник научных статей. В 3 т., Санкт-Петербург, 17–21 февраля 2025 года. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2025. – С. 456-459. – EDN PVOYXT.
8. Каримов, А. Р. Эндемическое равновесие в расширенной SEIR модели / А. Р. Каримов, М. А. Соломатин // Ядерная физика и инжиниринг. – 2025. – Т. 16, № 2. – С. 254-258. – DOI 10.56304/S2079562925020022. – EDN CUQQVM.

УДК 004.056

#### МОДЕЛЬ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОЛЬЗОВАТЕЛЯ СОЦИАЛЬНОЙ СЕТИ

**Борисов Сергей Валерьевич**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича  
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mail: sergeiborisov@ieee.org

**Аннотация.** В данной работе предложена авторская модель цифровой устойчивости пользователя в социальных сетях. Модель отражает оценку устойчивости пользователя социальной сети к угрозам информационной безопасности, отражая такие составляющие, как взаимодействие с контентом, социальные связи пользователя и уровень текущих технических мер защиты от угроз информационной безопасности. На их основе вводится индекс, позволяющий оценить способность пользователя противостоять угрозам информационной безопасности в пространстве социальных сетей.

**Ключевые слова:** модель цифровой устойчивости; безопасность пользователя; социальные сети; информационная безопасность; индекс цифровой устойчивости.

#### A MODEL OF INFORMATION SECURITY THREATS FOR SOCIAL NETWORK USERS

**Borisov Sergei**

St Petersburg State University of Telecommunications named after Prof. M. A. Bonch-Bruевич  
22 Bol'shevikov Av., build. 1, St-Petersburg, 193232, Russia  
e-mail: sergeiborisov@ieee.org

**Abstract:** This paper proposes a proprietary model of user digital resilience on social media. The model assesses a social network user's resilience to information security threats, reflecting components such as interaction with content, the user's social connections, and the level of current technical measures to protect against information security threats. Based on these factors, an index is introduced to assess the user's ability to resist information security threats in the social media space.

**Keywords:** digital resilience model; user security; social networks; information security; digital resilience index.

В исследованиях уделяют внимание технической защите информации на пользовательском уровне [1], фишингу в интернет-пространстве [2]. Проводятся современные исследования и поиска бот-взаимодействий в социальных сетях. Внимание уделяется такому направлению, как противодействию кибербуллингу [3] в социальных сетях, исследование бот-активностей [4]. Также, в настоящее время существует острая проблема распространения контента, созданного с помощью технологий искусственного интеллекта [5].

Анализ релевантной литературы показал, что информационной безопасности пользователя социальной сети уделяется тщательное внимание. Однако, текущие исследования не рассматривали данный вопрос как единое целое. Таким образом, исходя из современной научной ситуации, ИБ пользователя в пространстве социальных сетей, безусловно, является актуальной проблемой.

Угрозы ИБ пользователей в социальных сетях. Современные научные исследования направлены на определенные способы решения проблем, однако данные способы сегментируют риски и рассматривают их порознь. Учитывая особенности платформ социальных сетей, определим группы угроз ИБ:

1. угрозы уровня технической защиты информации;
2. угрозы информационного уровня;
3. угрозы уровня социального взаимодействия.

Для решения проблемы обеспечения безопасности пользователя социальной сети предлагается авторская модель цифровой устойчивости пользователя социальной сети к угрозам информационной безопасности, объединяющая описанные выше подходы.

Данная модель представляет собой индекс цифровой устойчивости пользователя социальной сети к угрозам информационной безопасности в социальных сетях.

Обозначим тип технических угрозы как *technical*, социальные за *social*, угрозы контента как *content*, *user* – пользователь.

Распределение угроз по группам:

1.  $G_{user\,technical}(t)$  – группа технических угроз пользователя;
2.  $G_{user\,social}(t)$  – группа угроз социального взаимодействия пользователя;
3.  $G_{user\,content}(t)$  – группа угроз взаимодействия пользователя с контентом.

Определим цифровую устойчивость пользователя индексом *Resilience*. Тогда модель цифровой устойчивости будет иметь следующий вид:

$$Resilience_{user}(t) = f(G_{user\,technical}(t), G_{user\,social}(t), G_{user\,content}(t), W),$$

где:  $t$  – время,  $W$  – множество весовых коэффициентов типов угроз. На данном этапе весовые коэффициенты для каждой группы предлагает определять экспертным способом.

Целевая функция задачи повышения ИБ определяется как максимизацию индекса:  $Resilience_{user} \rightarrow max$ .

Представленная модель является новым научным результатом, выраженным в оценке устойчивости пользователя к угрозам информационной безопасности. Модель объединяет три уровня угроз информационной безопасности пользователя социальной сети: уровень контента, технический и социальный. Определена целевая функция максимизации индекса  $Resilience(u, t)$ .

Дальнейшими направлениями исследования являются предложение архитектурного решения для использования предложенного индекса, предложения по его внедрению, методика количественной оценки цифровой устойчивости пользователя социальной сети к угрозам информационной безопасности, а также совершенствование защиты пользователя от угроз.

## СПИСОК ЛИТЕРАТУРЫ

1. Тумбинская, М. В. Обеспечение защиты от нежелательной информации в социальных сетях / М. В. Тумбинская // Вестник Мордовского университета. – 2017. – Т. 27, № 2. – С. 264-288. – DOI 10.15507/0236-2910.027.201702.264-288. – EDN YPJOJL;
2. Борисов, С. В. Определение признаков фишинговых сообщений в электронной почте / С. В. Борисов, В. А. Севостьянов, А. Ю. Цветков // Студенческая весна - 2023 : Материалы 77-ой региональной научно-технической конференции студентов, аспирантов и молодых ученых, Санкт-Петербург, 23–24 мая 2023 года. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2023. – С. 88-92. – EDN OEBILD.
3. Виткова, Л. А. Методика противодействия кибербуллингу в социальных сетях / Л. А. Виткова // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2021. – № 4. – С. 49-54. – DOI 10.46418/2079-8199\_2021\_4\_7. – EDN PGJFSE.
4. Борисов, С. В. Боты в социальных сетях / С. В. Борисов, А. А. Мосиян, Д. В. Сахаров // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2024) : Сборник научных статей XIII Международной научно-технической и научно-методической конференции, Санкт-Петербург, 27–28 февраля 2024 года. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2024. – С. 560-563. – EDN YBALCT.
5. Борисов, С. В. Актуальность проблемы выявления сгенерированного видео с использованием технологий искусственного интеллекта в социальных сетях и цифровых медиа / С. В. Борисов // Безопасные информационные технологии : Сборник трудов Тринадцатой международной научно-технической конференции, Москва, 30 октября – 01 2024 года. – Москва: МГТУ им. Н.Э.Баумана, 2024. – С. 42-45. – EDN IMJYMW.



УДК: 004.056

**СОЦИОКОМПЬЮТИНГ И АУДИАЛЬНЫЕ КОММУНИКАЦИИ:  
КАК ЗАЩИЩАТЬ ГОЛОС В ЦИФРОВОЙ СРЕДЕ****Денисова Ольга Сергеевна**

Российский государственный педагогический университет им. А. И. Герцена  
реки Мойки наб., 48, Санкт-Петербург, 191186, Россия  
Открытая (сменная) общеобразовательная школа г. Онеги  
Пр. Гагарина, 48, г. Онега, Архангельская область, 164840, Россия  
e-mail: olganum@gmail.com

**Аннотация.** В статье исследуются голосовые коммуникации в цифровой среде через призму социокomпьютинга, их значение для идентификации пользователей и возникающие угрозы информационной безопасности. Особое внимание уделено голосовой биометрии, технологиям синтеза речи и голосовым дипфейкам. Рассматриваются комплексные меры защиты аудиальных данных — технологические, образовательные и социально-культурные.

**Ключевые слова:** социокomпьютинг; голосовая биометрия; идентификация по голосу; голосовые дипфейки; информационная безопасность; синтез речи; цифровая среда.

**SOCIOCOMPUTING AND AUDIO COMMUNICATIONS: HOW TO PROTECT  
THE VOICE IN THE DIGITAL ENVIRONMENT****Denisova Olga**

Herzen State Pedagogical University of Russia  
48 Moika River Emb., St. Petersburg, 199406, Russia  
Open (shift) secondary school in Onega  
48 Gagarin Ave, Onega, Arkhangelsk region, 164840, Russia  
e-mail: olganum@gmail.com

**Abstract.** The article explores voice communications in the digital environment through the lens of sociocomputing, their significance for user identification, and the emerging information security threats. Special attention is given to voice biometrics, speech synthesis technologies, and voice deepfakes. Comprehensive measures for protecting audio data are discussed, including technological, educational, and socio-cultural approaches.

**Keywords:** sociocomputing; voice biometrics; speaker identification; voice deepfakes; information security; speech synthesis; digital environment.

Социокomпьютинг как область знания изучает взаимодействие человека и цифровых систем, социальные процессы и коллективное поведение в сетевой среде. В последние годы становятся повседневностью голосовые чаты, подкасты, голосовые ассистенты, системы дистанционного обучения и биометрическая аутентификация.

Голос — это не просто средство общения. Он одновременно является личностным маркером, биометрическим ключом и социальным инструментом доверия. Именно поэтому аудиальные коммуникации становятся новой ареной для угроз информационной безопасности.

Уникальность голосовой биометрии заключается в том, что это «единственная биометрическая модальность, которая позволяет идентифицировать человека по телефону [1-4]. Использование голоса для аутентификации всё шире применяется при использовании различных услуг, в криминалистике, в банковских сервисах, телекоммуникациях и государственных услугах. Уникальные характеристики речи — тембр, ритм, интонация — формируют своеобразный «цифровой отпечаток». Голос делает уникальным его физиологические особенности. Однако в отличие от пароля или токена голос невозможно «сменить», если он оказался скомпрометирован. Это делает защиту аудиальных данных особенно актуальной.

Современные технологии синтеза речи (например, Text-to-Speech, VoiceCloning) позволяют воспроизвести голос конкретного человека всего по нескольким минутам записи. В результате злоумышленники получают возможность обходить системы биометрической аутентификации, совершать мошеннические звонки от имени знакомых, коллег или официальных структур, распространять дезинформацию через аудиальные каналы, включая социальные сети и мессенджеры. Угроза кражи голоса выходит за рамки частной безопасности и становится социальным вызовом, влияющим на доверие к цифровым коммуникациям.

Социокomпьютинг рассматривает цифровую среду как систему, где взаимодействие людей и алгоритмов формирует новые формы поведения и коммуникации. В этой логике голосовые каналы приобретают особое значение. В образовании дистанционные лекции, онлайн-курсы и тьюторские платформы опираются на голосовое взаимодействие. Подкасты и аудиоблоги в культуре и медиа становятся формой коллективного знания и обмена опытом. В повседневной жизни голосовые помощники и умные устройства собирают и анализируют речь пользователей. Во всех этих случаях аудиальные коммуникации формируют новые социальные практики, но одновременно создают риски сбора и утечки биометрических данных.

Основными угрозами становятся

- голосовые дипфейки (синтезирование речи, неотличимой от живого голоса),

- утечка биометрических данных (получение доступа злоумышленников к уникальным биометрическим ключам),
- манипуляции через звук (применение аудиального канала для распространения слухов, фейков и психологического давления),
- незаметный сбор данных (фиксирование речи голосовыми помощниками и «умными» устройствами).

Для защиты аудиальных данных нужны технологические меры: алгоритмы детектирования синтезированного голоса, защищённые протоколы передачи и хранения, а также многофакторная аутентификация, где голос используется только как дополнительный идентификатор.

Образовательные меры включают внедрение модулей по аудиальной безопасности и медиаграмотности, развитие навыков распознавания аудио-фейков у пользователей и применение игровых и иммерсивных методов обучения с синтезаторами и саунд-дизайном для моделирования атак.

Культурные и социальные меры включают привитие осторожного отношения к биометрическим данным, использование звуковых сигналов для предупреждения об угрозах и объединение специалистов для совместной работы над безопасными цифровыми решениями [5].

Социокомпьютинг показывает, что цифровая среда — это не только текст и изображение, но и сложные аудиальные коммуникации. (Отметим, в частности, что на таком подходе основана разработка интеллектуальной системы каталогизации музыки народов России и мира (см. подробнее в работах [5-7]), создаваемая сотрудниками научно-методической лаборатории «Музыкально-компьютерные технологии» Российского государственного университета им. А. И. Герцена.)

Голос становится новым «цифровым паспортом», объединяющим личность и её социальное присутствие. Угроза кражи голоса и биометрических данных требует комплексного подхода: технологического, образовательного и культурного. Только в этом случае можно сохранить доверие к цифровым сервисам и обеспечить безопасность человека в условиях стремительно развивающегося социокомпьютинга.

#### СПИСОК ЛИТЕРАТУРЫ

1. Задорожный В.В. Обзор биометрических технологий // Защита информации. Конфидент. 2003. № 5. С. 26–29.
2. Зубалова О. А. Проблемы информационной безопасности образовательной среды в современных условиях [Электронный ресурс] // Научная электронная библиотека «КиберЛенинка» URL: <https://cyberleninka.ru/article/n/problemy-informatsionnoy-bezopasnosti-obrazovatelnoy-sredy-v-sovremennyh-usloviyah> (дата обращения: 13.09.2025). С. 36-38.
3. Мамырбаев О.Ж., Кыдырбекова А.С., Ахмедиярова А.Т., Турдалыұлы М., Мекебаев Н.О. Систематический обзор и анализ особенностей идентификации по голосу // Вестник Казахстано-Британского технического университета. 2019. Т. 16, № 2. С. 120–133.
4. Матвеев Ю.Н. Технологии биометрической идентификации личности по голосу и другим модальностям [Электронный ресурс] // Academia.edu. URL: <https://yagla.tv/cXskrqB> (дата обращения: 13.09.2025).
5. Матвеев Ю.Н., Симончик К.К. Система идентификации дикторов по голосу для конкурса NIST SRE 2010 // ГрафиКон'2010. Труды 20-й Междунар. конф. по компьютерной графике и зрению. СПб: СПбГУ ИТМО, 2010. С. 315–319.
6. Горбунова И.Б., Алиева И.Г. О проекте создания интеллектуальной системы по каталогизации и анализу музыки народов мира // Общество: философия, история, культура. 2016. № 9. С. 105-108.
7. Горбунова И.Б., Алиева И.Г. К проблематике разработки интеллектуальной системы каталогизации музыки народов России и мира. Трансдисциплинарный подход к изучению музыкальных явлений: теория нечётких множеств // В сборнике: Региональная информатика и информационная безопасность. Сборник трудов Санкт-Петербургской международной конференции и Санкт-Петербургской межрегиональной конференции. Санкт-Петербург, 2024. С. 316-319.

УДК 004.031.4

#### ЛОГИСТИЧЕСКИЙ ПОРТАЛ CARGOTIME.RU: МЕТОДЫ УНИФИКАЦИИ ГЕОДАННЫХ КОНТЕЙНЕРНОЙ ПЕРЕВОЗКИ

Есин Максим Сергеевич, Корепанова Анастасия Андреевна, Сазанов Вадим Алексеевич  
СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия  
e-mail: mse@dscs.pro, aak@dscs.pro, vas@dscs.pro

**Аннотация.** В работе представлен сравнительный анализ двух подходов к унификации геолокаций контейнерных маршрутов: локального геокодера на основе данных OpenStreetMap и внутреннего справочника портов и станций. Оценка проводилась по критериям качества данных, времени отклика, устойчивости и стоимости. Показано, что внутренний справочник обеспечивает более высокую точность и скорость работы при минимальных затратах, а также позволяет использовать отраслевые стандарты кодирования. Описана архитектура хранилища геоданных, включающая сущности локаций, стран и регионов, а также механизмы поддержки локализации и расширяемости. Представленные результаты демонстрируют практическую значимость применения внутреннего справочника для обеспечения согласованности и надежности логистических данных в цифровых сервисах контейнерного трекинга.

**Ключевые слова:** хранение геоданных; унификация локаций; отслеживание контейнеров морских линий; веб-приложения.

LOGISTICS PORTAL CARGOTIME.RU: METHODS OF UNIFICATION  
OF CONTAINER TRANSPORTATION GEODATA  
Esin Maxim, Korepanova Anastasya, Sazanov Vadim

St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)  
39 14th Line St, Petersburg, 199178, Russia  
e-mail: mse@dscs.pro, aak@dscs.pro, vas@dscs.pro

**Abstract.** This paper presents a comparative analysis of two approaches to the unification of geolocations in container route data: a local geocoder based on OpenStreetMap data and an internally developed directory of ports and stations. The approaches are evaluated against four key criteria: data quality, response time, robustness, and operational cost. The analysis demonstrates that the internal directory ensures higher accuracy and faster performance at lower cost, while also supporting the integration of industry-specific coding standards. Furthermore, the paper outlines the architecture of the geodata repository, which incorporates entities for locations, countries, and regions, as well as mechanisms for localization and extensibility. The results highlight the practical relevance of adopting the internal directory as a means of achieving consistency and reliability in logistics data for digital container tracking services.

**Keywords:** geodata storage; location unification; tracking of shipping containers; web applications.

Эффективный контроль цепочек поставок, и особенно отслеживание морских контейнеров, является ключевым фактором современной логистики. Современные системы мониторинга предоставляют возможность наблюдать за грузом на протяжении всего маршрута — от момента погрузки на судно до получения его конечным адресатом. Такие решения делают доставку более прозрачной и предсказуемой для клиентов, а также позволяют оперативно реагировать на критические ситуации, например на повреждение или утрату контейнера, что способствует росту надежности перевозки [1].

Логистический портал Cargotime.ru [2], разработанный на базе лаборатории прикладного искусственного интеллекта СПб ФИЦ РАН, предоставляет инструмент для отслеживания контейнеров по 100 международным морским линиям и железнодорожным операторам через единый интерфейс. Для получения информации пользователю достаточно ввести трек-номер, после чего система автоматически отображает актуальные данные о контейнере, его текущем статусе и маршруте следования напрямую из информационных систем перевозчиков.

Важную роль в работе сервиса играет корректная интерпретация геоданных о морских портах и железнодорожных станциях, связанных с маршрутами контейнерных перевозок. Локации, указанные в ответах перевозчиков, могут быть в разных форматах и с использованием разных кодировок. Это затрудняет процесс сопоставления портов и станций с унифицированными наименованиями, что усложняет построение и отображение маршрутов.

Для устранения этих проблем необходим механизм унификации геоданных, который позволит автоматически приводить «сырые» данные к единому виду. В работе описываются два практических подхода: развертывание локального геокодера на базе OpenStreetMap [3] и поддержка внутреннего справочника логистических объектов, формирующегося из фактических названий локаций, встречающихся в ответах перевозчиков. Сравнимые подходы оценивались по следующим метрикам:

- качество данных — доля корректных распознаваний портов и станций;
- время отклика — задержка ответа при рабочей нагрузке;
- устойчивость — способность функционировать при нестабильной сети или пиковых запросах;
- стоимость — расходы на внедрение, инфраструктуру, поддержку и обновление.

Сравнительный анализ показал, что подход с реализацией внутреннего справочника обеспечивает более высокое качество данных, минимальное время отклика и сравнимую с аналогом устойчивость работы при низкой стоимости эксплуатации.

В работе рассматриваются архитектурные основы предложенного решения, описываются используемые стандарты и механизмы унификации, а также структура хранилища геоданных. Дополнительно показано, что внедрение внутреннего справочника позволило существенно повысить показатели покрытия геоданных: доля успешно унифицированных локаций в ответах перевозчиков выросла, что напрямую улучшило полноту и корректность информации о маршрутах. Эти результаты подтверждают эффективность предложенного подхода для последующего применения данных в аналитических и предиктивных задачах.

*Перспективы развития.* В дальнейшем планируется расширение справочника за счёт интеграции дополнительных стандартов и автоматизация обновления данных. Перспективным направлением является применение методов машинного обучения для интеллектуального сопоставления «сырых» локаций, а также развитие поддержки многоязычных интерфейсов. Эти шаги обеспечат масштабируемость решения и создадут основу для аналитических и предиктивных сервисов, связанных с построением маршрутов [4, 5].

*Благодарности.* Работа выполнена в рамках проекта по государственному заданию СПб ФИЦ РАН № FFZF□2025□0006.

## СПИСОК ЛИТЕРАТУРЫ

1. Yue Z., Mangan J. A framework for understanding reliability in container shipping networks // Maritime Economics & Logistics. 2023. doi: 10.1057/s41278-023-00269-7.
2. Информационный ресурс Cargotime [Электронный ресурс] URL: <https://cargotime.ru/> (дата обращения: 15.09.2025).
3. Nominatim — локальный универсальный геокодер на базе OpenStreetMap [Электронный ресурс] URL: <https://nominatim.org/> (дата обращения: 15.09.2025).
4. Золотых Д. А., Есин М. С., Корепанова А. А., Сабреков А. А. Автоматизация построения оптимального плана дозаправок вдоль автомобильного маршрута с учетом ограничения на число остановок // Международная конференция по мягким вычислениям и измерениям. 2024. Т. 1. С. 510-514.

5. Есин М. С., Абрамов М. В. Построение оптимального плана дозаправок с использованием агрегированных сведений о значениях параметров маршрута из открытых источников // Научно-технический вестник информационных технологий, механики и оптики. 2025. Т. 25, № 4. С. 780-788. DOI 10.17586/2226-1494-2025-25-4-780-788.

УДК 004.056.5

## МЕТАМОДЕЛИ И МЕТРИКИ УСТОЙЧИВОСТИ СОЦИОКОМПЬЮТИНГА К ИНФОРМАЦИОННЫМ ИСКАЖЕНИЯМ

Изотов Даниил Юрьевич, Яровой Роберт Владимирович

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: daniil.izotov.1999@mail.ru, Nadzar@yandex.ru

**Аннотация.** В тезисе рассмотрены модели распространения фейков, метрики устойчивости, способы детектирования и стратегические подходы к снижению уязвимости. Представлены эпидемические и графовые симуляции, а также практики архитектурной перестройки.

**Ключевые слова:** дезинформация; социокмпьютинг; фейки; устойчивость сети; инфоэпидемия; графовая модель; TrustRank; ретрансляция; контент-боты.

## METAMODELS AND METRICS OF SOCIOCOMPUTING RESILIENCE TO INFORMATION DISTORTIONS

Izotov Daniil, Yarovoy Robert

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: daniil.izotov.1999@mail.ru, Nadzar@yandex.ru

**Abstract.** The thesis examines fake distribution models, resilience metrics, detection methods, and strategic approaches to reducing vulnerability. Epidemic and graph simulations are presented, as well as architectural restructuring practices.

**Keywords:** disinformation; sociocomputing; fakes; network stability; infoepidemic; graph model; TrustRank; retransmission; content bots.

Цифровая среда больше не нейтральна: она стала площадкой, где дезинформация распространяется не хаотично, а согласно закономерностям, укоренённым в архитектуре взаимодействий и алгоритмических предпочтениях. Социокмпьютинговые системы — совокупность технической, поведенческой и семантической динамики — оказываются уязвимыми не узловыми точками, а связями между ними [1].

Фейки и дезинформация становятся управляемыми агентами, воспроизводимыми через интерфейсы, алгоритмы ранжирования, ретрансляционные петли и системы доверия. Каскадный эффект мультиплицируется за счёт вовлечения: лайки, репосты и комментарии работают как маркеры легитимности [2].

Анализ устойчивости строится на трёх уровнях: техническом, поведенческом и метауровневом. Используются эпидемические модели (SIR, SEIR), агентные симуляции и графовые схемы. Метрики включают пороги устойчивости, среднее время насыщения, долю заражённых узлов, индексы ретрансляционной активности. Гетерогенность и фрагментация графа оказываются факторами устойчивости, затрудняя лавинообразное распространение [3].

Наиболее продуктивны композитные модели устойчивости, сочетающие статистику, поведение и структуру. Поведенческая аномальность выявляется через алгоритмический мониторинг активности: всплески, повторяемость, синхронность публикаций. Контент-боты и нейросетевые генераторы требуют не блокировки, а стратегий нейтрализации — снижение видимости, шумовые искажения, изоляция траекторий [4].

Ключевыми мерами являются ансамбли моделей детекции — лексических, контекстуальных и графовых, алгоритмы репутации, включая TrustRank и динамическую оценку источников, архитектурные перестройки интерфейсов и систем ранжирования, внедрение рефлексивных и когнитивных фильтров.

Только комплексное сочетание фильтрации, детекции, репутации и просвещения может выработать сетевой иммунитет. Эффективная защита — это не блокировка, а архитектурная настройка среды, делающая распространение фейка нерентабельным и самоуничтожающимся.

## СПИСОК ЛИТЕРАТУРЫ

1. Солодун Б.В., Рябов Г.А., Боголепов Г.С., Яровой Р.В. Подход к решению задачи оптимального выбора программных средств защиты информации в автоматизированных системах управления // Национальная безопасность России: актуальные аспекты. Сборник избранных статей Всероссийской научно-практической конференции. СПб, 2021. С. 31-36.
2. Михайлов Д.А. Использование актуальных оптимизаторов нейронных сетей в задачах социокмпьютинга // Региональная информатика (РИ-2024). Материалы XIX Санкт-Петербургской международной конференции. Санкт-Петербург, 2024. С. 388-389.
3. Овчаренко В.С., Синоюшкина С.Е. Проблемы борьбы с дезинформацией и фейками в современном информационном пространстве // Современные исследования: теория и практика. Сборник статей VII Международной научно-практической конференции. Петрозаводск, 2024. С. 259-263.
4. Слесарева А.М., Фролова Т.Н. Критическое мышление в эпоху дезинформации и фейков // Проблемы патриотического воспитания сотрудников правоохранительных органов и противодействия идеологии неонацизма и экстремизма. Сборник научных трудов. Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя и др., РУС, 2023. С. 237-239.

УДК 51.76

**СЦЕНАРНОЕ МОДЕЛИРОВАНИЕ ЭКСТРЕМАЛЬНОГО РАЗВИТИЯ ВОЛН ИНФОРМАЦИОННЫХ АТАК В ВОЗМУЩЕННОМ СОЦИОИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ****Переварюха Андрей Юрьевич**

СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия

email: madelf@rambler.ru

**Аннотация.** В ходе исследований развивалась методология представления комбинированного набора сравнительных вычислительных сценариев на основе представления вариативной и событийно перестраиваемой гибридной структуры уравнений, отражающей формы развития и затухания информационных потоков при целевом возмущении среды распространения и эффекта поляризации общества. При формировании атаки с целью дестабилизации поведения целевой группы сообщества и проведения тактики «информационных вбросов» реализуются хаотические переходные режимы динамики состояния векторного поля индивидуальных поведений, которые вызывают с запаздыванием ответную реакцию демпфирования, вызывая серию затухающих волн.

**Ключевые слова:** гибридные структуры; волны потоков информации; модель кибератаки.

**SCENARIO MODELING OF EXTREME DEVELOPMENT OF INFORMATION ATTACK WAVES IN A DISTURBED SOCIO-INFORMATION SPACE****Perevaryukha Andrey**

St. Petersburg Federal Research Center of the Russian Academy of Sciences

39 14th Line VO, St. Petersburg, 199178, Russia

email: madelf@pisem.net

**Abstract.** This research developed a methodology for presenting a combined set of comparative computational scenarios based on the presentation of a variable and event-reconfigurable hybrid structure of equations, reflecting the forms of development and attenuation of information flows with a target disturbance of the propagation environment and the effect of polarization of society. When forming an attack with the purpose of destabilizing the behavior of the target group of the community and conducting the tactics of «information injections», chaotic transient modes of the dynamics of the state of the vector field of individual behaviors are realized, which cause a delayed response of damping, causing a series of fading waves.

**Keywords:** hybrid structures; waves of information flows; cyber-attack model.

Гибридные методы сценарного моделирования требуются для анализа взрывообразных стадий развития информационных процессов при эффектах вбросов в современном социуме при замедленной реакции регулирующих организаций. Гибридные вычислительные структуры призваны решать актуальные задачи прогнозирования, качественной и количественной оценки последствий и выработке методов противодействия явлению вторжения целенаправленной деструктивной информации, имеющей тенденцию к неконтролируемому распространению в создавшихся условиях. Смена фаз генезиса и формализация масштабных нестационарных состояний в информационных потоках, к которым относится подавляющее большинство деструктивных информационных вбросов, одновременно одна из актуальных нерешенных проблем для математической социологии как междисциплинарного научного направления. При формализации социологии кибератак постановка задачи формального описания стремительных изменений в информационной динамике у разных общественных групп влияния представляет теоретический интерес из-за необходимой модификации представлений о действующих механизмах и о диапазонах их действия и исключения, в регуляции эффективности передачи волны сообщений в различных состояниях настроения общества и групп [1, 2].

Процесс распространения волны информационного вброса сравним с агрессивной инвазией. Экстремальность трендов у новых популяций вселенцев зависит от уровня сопротивления биотического окружения. Многие наблюдаемые ситуации при массовых размножениях связаны с явлениями инвазий и адаптаций чужеродных видов перманентной современной проблемой. В некоторых случаях вид-вселенец, представленный изначально малой группой особей, не встречает конкурентного противодействия со стороны автохтонного биологического окружения. Тогда у образующейся популяции происходит максимизация репродуктивного потенциала, который на самом деле является агрегированной и отнюдь не независимой характеристикой. Данная характеристика должна включать запаздывание в регуляции. Инвазия далеко не всегда переходит в стадию вспышки. В некоторых случаях инвазия может оказаться даже полезной для питания ценных потребителей, как в случае с донной фауной Каспийского моря, где проникновение средиземноморских моллюсков повысило продуктивность кормовой биомассы рыб во время падения уровня моря. Вспышки численности свойственны и неизмеримо давно присутствующим в экосистеме видам. В некотором смысле они становятся частью круга последовательных перестроений в растительных сообществах. О цикличности или стохастичности причин таких явлений ведется длительная дискуссия. Можно сделать вывод о действии пороговых состояний численности при сложном межвидовом взаимодействии группы видов, составляющих трехуровневую систему противоборства паразитов и их жертв. Аналогичные адаптивные волны формирует волна хайпа в плотных сообществах сети Internet [3].

Основной аспект, выделяемый нами в комплексной проблеме исследования вспышек в том, что по-видимому, нереально выделить общий путь развития процесса именно с позиций теории метаморфозов фазовых портретов

нелинейных динамических систем, аппарата для описания резких изменений. Данные ряда примеров указывают на различия в типах бифуркаций. Наиболее оправданным видится сценарный подход к моделированию ситуаций с некоторым множеством вариантов дальнейшего развития. Волны атак затухают после пика разными путями и иногда с последствием и реактивацией конфликта. В настоящей работе мы предлагаем непрерывную модель бифуркационного запуска сценария специфически осциллирующей вспышки на основе концепции запаздывания в действии регулирующих факторов. Модельный сценарий актуален по имеющимся данным наблюдений для случаев поражения вредителем лесов Канады и позволяет оценивать временную эволюцию характеристик пилообразных колебаний численности [4].

Традиционными методами математической экологии описать нелинейность завершения и спонтанность выхода из хаотических флуктуаций представлялось невозможным. Был выбран подход в форме непрерывно-дискретной динамической системы, строившейся на формализации выживаемости поколения. Изменения непрерывной системы в выделенные условиями моменты времени были соотнесены с переходами между тремя стадиями развития онтогенеза псиллид, для каждой из стадий отличаются факторы зависящей от плотности смертности, как и независимой.

Непрерывная часть базовой модели для  $N(t)$  описывалась переопределяемой правой частью дифференциального уравнения для убыли численности на трех последовательных временных интервалах с набором условий завершения активности и перехода к расчету смежного поколения [2, 5].

Таким образом, мы получили сложную зависимость для дискретной составляющей траектории, которая демонстрирует спонтанное преодоление порогового равновесия из переходного хаотического режима. Изначально при анализе наблюдений предполагалась вариативность на стадии завершения вспышки, что не было учтено нами в предыдущей статье, но вполне можно отразить в модели просто уменьшив вклад функционала, индуцирующего тут эффект Аллее. Для описания завершения вспышки инкапсулирован триггерный функционал. Он редуцирует притягивающую стационарную точку  $R^*$ , что резко переведет популяцию в следующий период хаотических флуктуаций. Порог запуска вспышки  $L$  не может быть монотонно достижим из любого состояния системы, все же вспышка численности с дефолиацией — это эпизодическое явление, потому несвязные границы областей притяжения аттракторов в нашей модели хорошо описывают данный экологический аспект. Существование порога, отраженного в модели граничным неустойчивым положением равновесия, объясняется сложными взаимоотношениями различных видов паразитических наездников. Полученные модели можно использовать в составе систем уравнений явного межвидового противоборства, они вычислительно значительно более сложны, чем современные модели трофодинамики «хищник-жертва», но обладают качественным разнообразием поведения у дискретных итераций.

Вспышки автохтонных видов менее разнообразны по аспектам прохождения фаз, чем экстремальные варианты развития инвазионного процесса, потому полученные имитационные сценарии не исчерпывают всю возможную динамику. Особенно интересны различия, если посмотреть на хорошо документированные явления в экосистемах через призму математической теории динамических систем. Полученный в уравнении переходный режим рассмотрим так же для задачи анализа случая специфического развития рецидивирующей инфекции. Интересно дальнейшее расширение уравнений для модельных исследований инвазионных процессов других видов со сложным независимым противодействием. Спровоцировать следующую серию колебаний с уровня информационных потоков в такой модели может стремительные изменения состояния общественных настроений. В дальнейшем развитии модели информационных атак нами планируется описание осциллирующей пилообразной динамики информационных волн из-за рецидивов активации интереса к деструктивной информации со стороны активных групп влияния в целевой среде и давления из вне.

#### СПИСОК ЛИТЕРАТУРЫ

1. Дубровская В. А. О критериях обоснованности для анализа нелинейных эффектов в моделях эксплуатируемых популяций // Проблемы механики и управления: Нелинейные динамические системы. 2016. № 48. С. 74-83.
2. Переварюха А. Ю. Модель развития спонтанной вспышки численности насекомого с аperiodической динамикой // Энтомологическое обозрение. 2015. Т. 94, № 1. С. 203-215.
3. Переварюха А. Ю. Хаотические режимы в моделях теории формирования пополнения популяций // Нелинейный мир. 2009. Т. 10, № 4. С. 925-932.
4. Переварюха А. Ю. Интерпретация поведения моделей динамики биоресурсов и моментальная хаотизация в новой модели // Нелинейный мир. 2012. Т. 10, № 4. С. 255-262.
5. Trofimova I. V., Manvelova A. B. Adequacy of interpretation of monitoring data on biophysical processes in terms of the theory of bifurcations and chaotic dynamics // Technical Physics Letters. 2022. Vol. 48. P. 305-310.

УДК 51.76

#### СЦЕНАРНОЕ МОДЕЛИРОВАНИЕ ЭКСТРЕМАЛЬНОГО РАЗВИТИЯ ВОЛН ИНФОРМАЦИОННЫХ АТАК В ВОЗМУЩЕННОМ СОЦИОИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Переварюха Андрей Юрьевич

СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия

email: madelf@rambler.ru

**Аннотация.** В ходе исследований развивалась методология представления комбинированного набора сравнительных вычислительных сценариев на основе представления вариативной и событийно перестраиваемой

гибридной структуры уравнений, отражающей формы развития и затухания информационных потоков при целевом возмущении среды распространения и эффекта поляризации общества. Нами при формировании атаки с целью дестабилизации поведения целевой группы сообщества и проведения тактики «информационных вбросов» реализуются хаотические переходные режимы динамики состояния векторного поля индивидуальных поведений, которые вызывают с запаздыванием ответную реакцию демпфирования, вызывая серию затухающих волн. Выделены два варианта развития волн информационного хайпа и HR-атаки.

**Ключевые слова:** гибридные структуры; волны потоков информации; модель кибератаки.

## SCENARIO MODELING OF EXTREME DEVELOPMENT OF INFORMATION ATTACK WAVES IN A DISTURBED SOCIO-INFORMATION SPACE

Perevaryukha Andrey

St. Petersburg Federal Research Center of the Russian Academy of Sciences

39 14th Line VO, St. Petersburg, 199178, Russia

email: madelf@rambler.ru

**Abstract.** In the course of the research, a methodology for presenting a combined set of comparative computational scenarios was developed based on the presentation of a variable and event-reconfigurable hybrid structure of equations reflecting the forms of development and attenuation of information flows with a target disturbance of the propagation environment and the effect of polarization of society. When forming an attack with the purpose of destabilizing the behavior of the target group of the community and conducting the tactics of «information injections», we implement chaotic transient modes of the dynamics of the state of the vector field of individual behaviors, which cause a delayed response of damping, causing a series of fading waves. Two variants of the development of waves of information hype and HR attacks are identified.

**Keywords:** hybrid structures; waves of information flows; cyber-attack model.

Гибридные методы сценарного моделирования требуются для анализа взрывообразных стадий развития информационных процессов при эффектах вбросов в современном социуме при замедленной реакции регулирующих организаций. Гибридные вычислительные структуры призваны решать актуальные задачи прогнозирования, качественной и количественной оценки последствий и выработке методов противодействия явлению вторжения целенаправленной деструктивной информации, имеющей тенденцию к неконтролируемому распространению в создавшихся условиях. Смена фаз генезиса и формализация масштабных нестационарных состояний в информационных потоках, к которым относится подавляющее большинство деструктивных информационных вбросов, одновременно одна из актуальных нерешенных проблем для математической социологии как междисциплинарного научного направления. При формализации социологии кибератак постановка задачи формального описания стремительных изменений в информационной динамике у разных общественных групп влияния представляет теоретический интерес из-за необходимой модификации представлений о действующих механизмах и о диапазонах их действия и исключения, в регуляции эффективности передачи волны сообщений в различных состояниях настроения общества и групп.

Процесс распространения волны информационного вброса сравним с агрессивной инвазией. Экстремальность трендов у новых популяций вселенцев зависит от уровня сопротивления биотического окружения. Многие наблюдаемые ситуации при массовых размножениях связаны с явлениями инвазий и адаптаций чужеродных видов перманентной современной проблемой. В некоторых случаях вид-вселенец, представленный изначально малой группой особей, не встречает конкурентного противодействия со стороны автохтонного биологического окружения. Тогда у образующейся популяции происходит максимизация репродуктивного потенциала, который на самом деле является агрегированной и отнюдь не независимой характеристикой. Данная характеристика должна включать запаздывание в регуляции. Инвазия далеко не всегда переходит в стадию вспышки. В некоторых случаях инвазия может оказаться даже полезной для питания ценных потребителей, как в случае с донной фауной Каспийского моря, где проникновение средиземноморских моллюсков повысило продуктивность кормовой биомассы рыб во время падения уровня моря. Вспышки численности свойственны и неизмеримо давно присутствующим в экосистеме видам. В некотором смысле они становятся частью круга последовательных перестроений в растительных сообществах. О цикличности или стохастичности причин таких явлений ведется длительная дискуссия. Можно сделать вывод о действии пороговых состояний численности при сложном межвидовом взаимодействии группы видов, составляющих трехуровневую систему противоборства паразитов и их жертв. Аналогичные адаптивные волны формирует волна хайпа в плотных сообществах сети Internet в условиях агрессивных атак кибертеррористов.

Основной аспект, выделяемый нами в комплексной проблеме исследования вспышек в том, что по-видимому, нереально выделить общий путь развития процесса именно с позиций теории метаморфозов фазовых портретов нелинейных динамических систем, аппарата для описания резких изменений. Данные ряда примеров указывают на различия в типах бифуркаций. Наиболее оправданным видится сценарный подход к моделированию ситуаций с некоторым множеством вариантов дальнейшего развития. Волны атак затухают после пика разными путями и иногда с последствием и реактивацией конфликта. В настоящей работе мы предлагаем непрерывную модель бифуркационного запуска сценария специфически осциллирующей вспышки на основе концепции запаздывания в действии регулирующих факторов. Модельный сценарий актуален по имеющимся данным

наблюдений для случаев поражения вредителем лесов Канады и позволяет оценивать временную эволюцию характеристик пилообразных колебаний численности.

Традиционными методами математической экологии описать нелинейность завершения и спонтанность выхода из хаотических флуктуаций представлялось невозможным. Был выбран подход в форме непрерывно-дискретной динамической системы, строившейся на формализации выживаемости поколения. Изменения непрерывной системы в выделенные условиями моменты времени были соотнесены с переходами между тремя стадиями развития онтогенеза псиллид, для каждой из стадий отличаются факторы зависящей от плотности смертности, как и независимой.

Непрерывная часть базовой модели для  $N(t)$  описывалась переопределяемой правой частью дифференциального уравнения для убыли численности на трех последовательных временных интервалах с набором условий завершения активности и перехода к расчету смежного поколения [2].

Таким образом, мы получили сложную зависимость для дискретной составляющей траектории, которая демонстрирует спонтанное преодоление порогового равновесия из переходного хаотического режима. Изначально при анализе наблюдений предполагалась вариативность на стадии завершения вспышки, что не было учтено нами в предыдущей статье, но вполне можно отразить в модели просто уменьшив вклад функционала, индуцирующего тут эффект Allee [3]. Для описания завершения вспышки инкапсулирован триггерный функционал. Он редуцирует притягивающую стационарную точку  $R^*$ , что резко переведет популяцию в следующий период хаотических флуктуаций. Порог запуска вспышки  $L$  не может быть монотонно достижим из любого состояния системы, все же вспышка численности с дефолиацией — это эпизодическое явление, потому несвязные границы областей притяжения аттракторов в нашей модели хорошо описывают данный экологический аспект. Существование порога, отраженного в модели граничным неустойчивым положением равновесия, объясняется сложными [4] взаимоотношениями различных видов паразитических наездников. Полученные модели можно использовать в составе систем [5-8] уравнений явного межвидового противоборства, они вычислительно значительно более сложны, чем современные модели трофодинамики «хищник-жертва», но обладают качественным разнообразием поведения у дискретных итераций [9-10].

Вспышки автохтонных видов менее разнообразны по аспектам прохождения фаз, чем экстремальные варианты развития инвазионного процесса, потому полученные имитационные сценарии не исчерпывают всю возможную динамику. Особенно интересны различия, если посмотреть на хорошо документированные явления в экосистемах через призму математической теории динамических систем. Полученный в уравнении переходный режим рассмотрим так же для задачи анализа случая специфического развития рецидивирующей инфекции. Интересно дальнейшее расширение уравнений для модельных исследований инвазионных процессов других видов со сложным независимым противодействием. Спровоцировать следующую серию колебаний с уровня информационных потоков в такой модели может стремительные изменения состояния общественных настроений. В дальнейшем развитии модели информационных атак нами планируется описание осциллирующей пилообразной динамики информационных волн из-за рецидивов активации интереса к деструктивной информации со стороны активных групп влияния в целевой среде и давления из вне.

#### СПИСОК ЛИТЕРАТУРЫ

1. Дубровская В.А. О критериях обоснованности для анализа нелинейных эффектов в моделях эксплуатируемых популяций // Проблемы механики и управления: Нелинейные динамические системы. 2016. № 48. С. 74-83.
2. Переварюха А.Ю. Модель развития спонтанной вспышки численности насекомого с аperiodической динамикой // Энтомологическое обозрение. 2015. Т. 94. № 1. С. 203-215.
3. Переварюха А. Ю. Хаотические режимы в моделях теории формирования пополнения популяций // Нелинейный мир. 2009. Т. 10, № 4. С. 925-932.
4. Переварюха А. Ю. Интерпретация поведения моделей динамики биоресурсов и моментальная хаотизация в новой модели // Нелинейный мир. 2012. Т. 10, № 4. С. 255-262.
5. Trofimova I. V., Manvelova A. B. Adequacy of interpretation of monitoring data on biophysical processes in terms of the theory of bifurcations and chaotic dynamics // Tech. Phys. Lett. 2022. Vol 48. P. 305-310.
6. Mikhailov V.V., Spesivtsev A.V., Perevaryukha A.Y. Evaluation of the dynamics of phytomass in the tundra zone using a fuzzy-opportunity approach // Studies in Computational Intelligence. 2020. Т. 868. С. 449-454.
7. Дубровская В.А., Переварюха А.Ю., Трофимова И.В. Модель динамики структурированных субпопуляций осетровых рыб Каспия с учетом отклонений в темпах развития молоди // Журнал Белорусского государственного университета. Биология. 2017. № 3. С. 76-86.
8. Соловьева Т.Н., Переварюха А.Ю. Динамическая модель деградации запасов осетровых рыб со сложной внутривидовой структурой // Информационно-управляющие системы. 2016. № 4 (83). С. 60-67.
9. Borisova T.Yu., Perevaryukha A.Yu. On the physicochemical method of analysis of the formation of secondary immunodeficiency as a bioindicator of the state of ecosystems using the example of seabed biota of the Caspian sea // Technical Physics Letters. 2022. Т. 48. № 7. С. 251-257.
10. Mikhailov V.V., Trofimova I.V. Computational modeling of the nonlinear metabolism rate as a trigger mechanism of extreme dynamics of invasion processes // Technical Physics Letters. 2022. Т. 48. № 12. С. 301-304.





## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

УДК 004.6, 004.051, 621.391

### ЭНЕРГОЭФФЕКТИВНОЕ И БЕЗОПАСНОЕ РАСПИСАНИЕ ПЕРЕДАЧИ ДАННЫХ В КИНЕМАТИЧЕСКИХ СЕНСОРНЫХ СЕТЯХ

Астахова Татьяна Николаевна

Нижегородский государственный инженерно-экономический университет

Октябрьская ул., 5, Княгинино, 606340, Россия

e-mails: ctn\_af@mail.ru

**Аннотация.** В статье предложена модель минимизации энергопотребления в кинематических сенсорных сетях, где устройства движутся по заранее заданным траекториям Дубинса. Представленная модель является интеграцией движения, энергии, необходимой для обеспечения информационной передачи и расписания передачи. Оптимизация сбора данных как стратегического ресурса требует не только эффективности, но и обеспечения его целостности, конфиденциальности и безопасности. Предложенная модель, уменьшая время и расстояние передачи, косвенно снижает векторы атаки (перехват, подслушивание, подмена), поскольку данные передаются в короткие, предсказуемые окна и только на минимально необходимое расстояние.

**Ключевые слова:** задача о назначениях; информационная безопасность; кинематическая сенсорная сеть; модель Дубинса; оптимизация расписания; формула Фрииса; экономика данных; энергопотребление; энергоэффективность.

### ENERGY-EFFICIENT AND SECURE DATA TRANSMISSION SCHEDULING IN KINEMATIC SENSOR NETWORKS

Astakhova Tatyana

Nizhny Novgorod State University of Engineering and Economics

22a Oktyabrskaya St, Knyaginino, 606340, Russia

e-mail: ctn\_af@mail.ru

**Abstract.** In the article, a model for minimizing energy consumption in kinematic sensor networks is proposed, where devices move along predefined Dubins paths. The presented model is an integration of motion, the energy required to support information transmission, and the transmission schedule. Optimizing data collection as a strategic resource requires not only efficiency but also ensuring its integrity, confidentiality, and security. The proposed model, by reducing the time and distance of transmission, indirectly lowers attack vectors (interception, eavesdropping, and tampering), since data are transmitted in short, predictable windows and only over the minimum necessary distance.

**Keywords:** assignment problem; information security; kinetic sensor network; schedule optimization; Dubins model; Friis transmission formula; data economy; energy consumption; energy efficiency.

Кинематические сенсорные сети с автономными устройствами сталкиваются с фундаментальной ограниченностью энергозапаса. В условиях динамических сред устройства, следуя заданным траекториям (например, дроны, роботы), могут использовать движение как инструмент энергосбережения, но также энергия необходима для обеспечения информационного взаимодействия устройств друг с другом и центром управления и мониторинга (ЦУОИ). Энергия радиопередачи, доминирующая по энергопотреблению, растёт пропорционально квадрату расстояния до базовой станции согласно уравнению Фрииса [1], поэтому передача данных в момент минимального расстояния является критически важной для энергоэффективности. Традиционные подходы, основанные на равномерном распределении временных окон, не учитывают этой динамики. Настоящая работа, опираясь на концепцию «Экономики данных», рассматривает данные как стратегический ресурс, управление которым требует комплексного подхода [2]. Повышение эффективности процесса сбора данных невозможно без обеспечения информационной безопасности: в цепочке передачи по беспроводному каналу основными угрозами являются перехват, прослушивание и подмена информации, и каждая передача может служить вектором атаки. Чем дольше и дальше распространяется сигнал, тем выше вероятность его компрометации. Следовательно, оптимизация расписания передачи, направленная на минимизацию дальности и времени передачи, является не только энергосберегающей, но и информационно безопасной стратегией. Сокращение временного окна и уменьшение радиуса передачи существенно ограничивают возможности атак и повышают устойчивость системы.

Идея общей модели — сочетание трех взаимосвязанных компонент: динамику движения, энергозатраты и расписание передачи, при этом безопасность встроена как требование к проекту, а не как отдельный слой. Цель такой модели — обеспечение эффективной передачи данных при минимальном энергопотреблении, но при этом сохранять устойчивость к угрозам и управляемость системой. Т.е. безопасность рассматривается не как второстепенное дополнение к энергоэффективности, а как неотъемлемая основа энергетически эффективной модели.

Модель движения (модель Дубинса) предполагает, что устройства перемещаются по оптимальным траекториям, состоящим из прямых участков и дуг окружностей, скорость устройств постоянна, радиус поворота ограничен, чтобы отражать реальные физические возможности движущихся устройств. Такая траектория обеспечивает предсказуемую динамику и ограниченную адаптивность к изменениям окружающей среды [3].

Модель энергозатрат (модель Фрииса) позволяет рассчитать мгновенную мощность передачи для  $i$ -го устройства в момент времени  $t$  в зависимости от расстояния  $d_i(t)$  до ЦУОИ по формуле Фрииса. Уменьшение передаваемой мощности снижает радиус распространения сигнала и, следовательно, вероятность перехвата несанкционированными субъектами. Механизм связывает энергопотребление с безопасностью: экономия энергии прямо влияет на крипто- и радио-обстановку.

Модель расписания и безопасности (задача назначения). Разделим временной цикл  $T$  на  $N$  окон: каждому устройству назначается ровно одно окно передачи. Целевая функция — минимизация суммарной мощности передачи:  $\min \sum \sum x_{ij} P_j(t_j)$  при ограничении, что каждое устройство передает один раз и каждое окно используется один раз.

Предсказуемое и детерминированное расписание позволяет ЦУОИ точно знать, когда и от какого устройства ожидать данные, что упрощает обнаружение подмен или аномалий (например, передачи от несуществующего устройства или в неверное окно). Конфиденциальность обеспечивается путем минимизации расстояния и времени передачи ограничивает зону потенциального перехвата. Очередность взаимодействия устройств, удаляющихся от ЦУОИ, обеспечивает передачу критически важных данных в первую очередь и снижает риск их потери или перехвата при дальнейшем удалении устройства. Предсказуемость и локализация передач снижают уязвимость системы к крупномасштабным атакам по сравнению с сетями с непрерывной или непредсказуемой передачей.

Интеграция безопасности в три компонента (динамика → энергозатраты → расписание) позволяет оптимизировать не только эффективность и энергопотребление, но и обнаружение нарушений и защиту информации на ранних стадиях проектирования системы.

Предложенная модель эффективно объединяет физические ограничения движения, реальные энергетические характеристики связи и математическую оптимальность расписания. Результаты эксперимента подтверждают высокую эффективность подхода, ориентированного на устройства, удаляющиеся от ЦУОИ, как ключевого фактора снижения энергозатрат. Ключевым вкладом работы является интеграция концепции информационной безопасности в основу энергоэффективной модели. Предлагается не просто способ сэкономить энергию, а безопасный способ сбора данных как стратегический ресурс. Сокращение расстояния и времени передачи является фундаментальным, а не второстепенным средством повышения безопасности. Этот подход позволяет существенно продлить срок службы автономных кинематических сенсорных сетей в приложениях умных городов, мониторинга окружающей среды и промышленной автоматизации, где надежность и защита данных являются критически важными. Дальнейшие исследования будут направлены на адаптацию модели для сетей с несколькими ЦУОИ, многокритериальной оптимизации и формализацию мер защиты на уровне протоколов связи.

#### СПИСОК ЛИТЕРАТУРЫ

1. Shaw, J. A.: Radiometry and the Friis transmission equation. American journal of physics № 81(1), С 33–37, 2013. <https://doi.org/10.1119/1.4755780>.
2. Астахова Т. Н., Колбанев М. О., Сущева Н. В., Шамин А. А. Экономика данных // International Journal of Open Information Technologies. 2024. Т. 12, № 10. С. 129-136.
3. Хабаров С. П., Шилкина М. Л. Геометрический подход к решению задачи для машин Дубинса при формировании программных траекторий движения // Научно-технический вестник информационных технологий, механики и оптики. 2021. Т. 21. №. 5. С. 653-663. <https://doi.org/10.17586/2226-1494-2021-21-5-653-663>.

УДК 004.056

#### ИДЕНТИФИКАЦИЯ ЛИЧНОСТИ С ИСПОЛЬЗОВАНИЕМ НЕПЕРЕДАВАЕМЫХ ТОКЕНОВ

Булгаков Дмитрий Алексеевич

Санкт-Петербургский государственный университет аэрокосмического приборостроения

Большая Морская ул., 67, Санкт-Петербург, 190121, Россия

e-mail: dmbulg@gmail.com

**Аннотация.** Отделение уникальных аккаунтов живых людей от дубликатов или ботов становится важной задачей для обеспечения правильного функционирования любого цифрового сервиса, предоставляющего какие-либо услуги пользователям, а также для справедливого распределения прав и защиты от мошеннических действий. Наибольшую опасность здесь представляют атаки Сивиллы, связанные с дестабилизацией работы сети при помощи множества подконтрольных учётных записей, и дипфейки, когда бот имитирует поведение реального человека. Были рассмотрены основные задачи, стоящие перед системой проверки идентичности, и

различные подходы к реализации таких систем, включая использование невзаимозаменяемых токенов для подтверждения уникальности аккаунта пользователя.

**Ключевые слова:** Доказательство личности; идентификация; NFT; SBT; блокчейн; атака Сивиллы.

## PROOF OF PERSONHOOD IMPLEMENTATION USING NON-TRANSFERABLE TOKENS

**Bulgakov Dmitry**

Saint Petersburg State University of Aerospace Instrumentation  
67, Bolshaya Morskaya St, St. Petersburg, 190121 Russia  
e-mail: dmbulg@gmail.com

**Abstract.** Separating unique accounts of living people from duplicates or bots is becoming an important task for ensuring the proper functioning of any digital service that provides any services to users, as well as for the fair distribution of rights and protection against fraudulent activities. The greatest danger here is posed by Sybil attacks associated with the destabilization of the network using multiple controlled accounts, and deepfakes, when a bot imitates the behavior of a real person. The main challenges facing the identity verification system and various approaches to the implementation of such systems were considered, including the use of non-fungible tokens to confirm the uniqueness of the user account.

**Keywords:** Proof of Personhood; identification; NFT; SBT; blockchain; Sybil attack.

По мере всё более глубокого проникновения цифровых агентов в жизнь человека возникает насущная потребность в эффективном способе проверки, кто находится перед вами: бот или человек [1]. Один из способов дифференциации людей и роботов — использование технологии «доказательства личности» (англ. Proof of Personhood, PoP) [2, 3], которая позволяет подтвердить личность человека в цифровом пространстве и отличить его от ИИ-агента. PoP сочетает несколько разных уровней верификации, например, объединяет уникальный код, присвоенный человеку, устройству или транзакции, с биометрическими данными. Помимо биометрии также может применяться проверка государственных документов или цифрового следа. При этом важное свойство PoP — сама личность при проверке не раскрывается. Для пользователя создаётся универсальный цифровой идентификатор для доступа к различным службам на основе блокчейна: DeFi, коллекциям NFT, dApp, системам онлайн-голосований. Также PoP помогает выявлять и блокировать пользователей, создающих множественные учётные записи для обхода ограничений сервиса или эксплуатации его функционала.

Стоит выделить две ключевые проблемы, для решения которых применяется PoP:

- защита от атак Сивиллы (англ. *Sybil attack*);
- защита от дипфейков.

Суть атаки Сивиллы заключается в получении контроля над большинством узлов одноранговой сети при помощи множества фальшивых идентичностей. Наибольшую опасность атаки Сивиллы представляют для различных систем электронного голосования и блокчейнов, использующих механизм валидации с доказательством хранения (англ. Proof of Stake, PoS) и игровых метавселенных, имеющих собственную экономическую модель [4].

В 2022 году создатель криптосети Ethereum Виталик Бутерин с коллегами предложил концепцию «привязанных к душе» (англ. Soulbound) токенов [6] (сокращённо SBT). Это особая разновидность NFT, который навсегда привязан к аккаунту (кошельку) пользователя, и который нельзя продать, передать или обменять. Такой NFT может служить доказательством не только личности человека, но и каких-либо его достижений: образования, членства в организациях, наград, сертификатов и т.д.

Для Soulbound-токенов в Ethereum были предложены специальные стандарты ERC-4973 и ERC-5192. Запрет на передачу токенов в первом реализован за счёт отсутствия функции transfer. Получается, что любой созданный токен остаётся закреплён за адресом (но не кошельком) пользователя до тех пор, пока эмитент не решит его аннулировать. Сфера применения ERC-4973 не ограничивается только SBT. Так, стандарт допускает, что владельцем токена может быть не только человек (EOA), но и смарт-контракт.

В минималистичном стандарте ERC-5192 для запрета на передачу токенов в код контракта добавляется специальное свойство locked. Если оно возвращает true, значит, данный токен заблокирован и не может быть передан другому аккаунту. Блокировка обратима и может быть снята автором контракта.

Классический стандарт ERC-721 не ограничивает владение NFT только EOA (реальными людьми). Наоборот, владельцем NFT или любого другого актива может быть как EOA, так и CA (другие смарт-контракты). Например, контракты децентрализованных маркетплейсов (OpenSea, Blur), мульти-кошельков или биржевых трейдерских ботов должны владеть NFT для выполнения своих функций. Тем не менее, существуют два способа искусственно ограничить возможность владения NFT ботами в коде смарт-контракта.

1. Добавить проверку, что вызывающий адрес — это EOA.
2. Сделать запрет на владение контрактами через проверку длины байт-кода.

Этот способ опирается на тот факт, что у EOA отсутствует байт-код, тогда как у CA он имеется. Значит, достаточно проверить длину строки кода. Она будет либо равна 0 для EOA, либо строго больше 0 для CA.

Код контракта SBT должен быть максимально оптимизированным и не содержать лишних функций и проверок, поскольку их выполнение увеличит плату за аренду вычислительных мощностей виртуальной машины Ethereum (т.н. «газ»).

Все токены стандарта ERC-4973 [7] характеризуются набором ключевых свойств: они неразрывно привязаны к одному аккаунту (адресу в сети Ethereum), не могут быть переданы на другой аккаунт, но могут быть выданы только с согласия владельца контракта, который также имеет право их отозвать (удалить с аккаунта).

Наиболее популярной сетью для SBT на данный момент является Polygon за счёт высокой скорости обработки транзакций и низких комиссий.

Представленный выше код создаёт контракт NFT, владелец которого может чеканить токены. У каждого токена свой уникальный ID, и эти токены нельзя передавать. При этом контракт знает, каким адресам уже был выдан токен, и запрещает выдавать токен повторно. При объявлении контракта указываются два словаря: первый хранит информацию о том, заблокирован ли токен, второй проверяет, был ли уже отчеканен токен на данный адрес.

После написания кода SBT-токена необходимо проверить следующие постулаты:

- SBT может быть отчеканен;
- SBT не может быть передан;
- один пользователь не может отчеканить SBT дважды;
- чеканить может только владелец контракта.

Такой SBT в перспективе может быть связан с прохождением CAPTCHA или верификацией в системах Worldcoin или Gitcoin Passport.

SBT-токены отлично подходят для построения системы доказательства знаний. Например, система, хранящая информацию об аттестатах, дипломах и индивидуальных заслугах человека, а также его рабочие резюме, включая участие в проектах и конкурсах.

Наибольшую тревогу на данный момент вызывает перспектива потери приватных ключей. Если пользователь не сможет получить доступ к своему основному кошельку (аккаунту), он также потеряет и все свои SBT. Для решения этой задачи предлагаются разные инициативы, например, «социальное восстановление» (англ. Social Recovery), когда пользователь заранее назначает доверенных лиц из числа друзей или членов семьи, или замена EOA на смарт-контракт с заранее заложенной логикой восстановления (например, через систему World ID). Эффективность и практическая применимость этих техник — задача для будущего исследования.

#### СПИСОК ЛИТЕРАТУРЫ

1. Adler S., Hitzig Z., Jain S., Brewer C. и др. Personhood credentials: Artificial intelligence and the value of privacy-preserving tools to distinguish who is real online. 10.48550/arXiv.2408.07892. 15 августа 2024 г.
2. Proof of personhood: What it is and why it's needed // Блог на сайте World ID [Электронный ресурс]. URL: <https://world.org/blog/world/proof-of-personhood-what-it-is-why-its-needed> (дата обращения: 25.08.2025).
3. Ohlhaber P., Nikulin M., Berman P. Compressed to 0: The Silent Strings of Proof of Personhood (March 6, 2024). Available at SSRN: <https://ssrn.com/abstract=4749892> or <http://dx.doi.org/10.2139/ssrn.4749892> (дата обращения: 25.08.2025).
4. Cao Y., Cao J., Liu H., Cui Z., Wen L. Eden: An Edge Computing Empowered Proof-of-Personhood Protocol for Anti-Sybil in Blockchain-based Metaverse. // The 2nd International Conference on Intelligent Metaverse Technologies & Applications (iMETA2024). 2024. DOI: 10.1109/iMETA62882.2024.10808133.
5. Lutz S. Ethereum Layer-2 Solution Optimism Loses 20 Million Tokens in Interlayer Snafu. Новость на сайте decrypt.co от 09.06.2022. URL: <https://decrypt.co/102377/ethereum-layer-2-solution-optimism-loses-20-million-tokens-in-interlayer-snafu> (дата обращения: 25.08.2025).
6. Ohlhaber P., Weyl E.G., Buterin V. Decentralized Society: Finding Web3's Soul. 2022. SSRN: <https://ssrn.com/abstract=4105763>. DOI: 10.2139/ssrn.4105763.
7. Daubenschütz T. ERC-4973: Account-bound Tokens. Обзор минималистичного стандарта для токенов, привязанных к аккаунту. URL: <https://eips.ethereum.org/EIPS/eip-4973> (дата обращения: 25.08.2025).

УДК 004.622

#### ЭФФЕКТИВНОСТЬ АТАК ПО СЛОВАРЮ

**Булгаков Дмитрий Алексеевич**

Санкт-Петербургский государственный университет аэрокосмического приборостроения

Большая Морская ул., 67, Санкт-Петербург, 190121, Россия

e-mail: [dmbulg@gmail.com](mailto:dmbulg@gmail.com)

**Аннотация.** Проведён обзор актуальных рекомендаций к парольной защите учётных записей пользователей с учётом социального фактора. Показано сравнение скорости взлома паролей, хешированных с помощью различных современных алгоритмов, с задействованием мощностей графического процессора. Предложен алгоритм составления комбинированного словаря парольных фраз, состоящего как из известных цитат, так и из случайных комбинаций действительных английских слов с учётом грамматики языка. Измерена скорость хеширования такого словаря на видеокarte RTX 4090 с использованием алгоритма SHA256.

**Ключевые слова:** пароли; атака перебором; атака по словарю; CUDA; хеширование; SHA256.

#### DICTIONARY ATTACK EFFICIENCY

**Bulgakov Dmitry**

Saint Petersburg State University of Aerospace Instrumentation

67, Bolshaya Morskaya St, St. Petersburg, 190121 Russia

e-mail: [dmbulg@gmail.com](mailto:dmbulg@gmail.com)

**Abstract.** A review of current recommendations for password protection of user accounts is conducted, taking into account the social factor. A comparison of the speed of cracking passwords hashed using various modern algorithms

is shown, using the power of the graphics processor. An algorithm for compiling a combined dictionary of password phrases is proposed, consisting of both known quotes and random combinations of real English words, taking into account the grammar of the language. The hashing speed of such a dictionary on the RTX 4090 video card using the SHA256 algorithm is measured.

**Keywords:** passwords; brute force attack; dictionary attack; CUDA; hashing; SHA256.

Для обработки паролей могут применяться различные алгоритмы хеширования, но все действуют схожим образом. Хеш-функция выполняет свёртку данных, т.е. преобразует входной массив («ключ») в битовую строку строго определённого размера («хеш-сумму») в соответствии с заданным алгоритмом. Процесс хеширования детерминирован и необратим. Это значит, что один и тот же пароль всегда будет иметь один и тот же хеш, и невозможно восстановить исходную строку из её хеша. Сам хеш записывается в защищённую базу данных на сервере. Отсюда «взлом» пароля — это не процесс расшифровки хеша, а создание собственного списка хешей и сравнение их с известными результатами.

В конце августа 2024 года Национальный институт стандартов и технологий США (NIST) выпустил второй черновик первоначального публичного проекта (IPD) стандарта SP 800-63-4 [1], относящегося к Руководству по цифровой идентификации (Digital Identity Guidelines). На основании отзывов и комментариев, собранных за 3 месяца от широкого круга заинтересованных организаций и лиц, Институт сформулировал набор технических требований и рекомендаций для аутентификации пользователей в интернете [2–4].

Помимо прочего, авторы документа заострили внимание на т.н. атаках в автономном режиме, которые становятся возможны, когда в результате взлома базы данных на руках у злоумышленника оказывается огромный список хешей паролей разных пользователей. Перед злоумышленником встаёт задача — восстановить исходный пароль из хеша. Согласно принципу Дирихле, однозначного соответствия между выходными данными хеш-функции и исходным паролем не существует, поэтому математическими методами восстановить пароль из хеша невозможно. Однако можно взять список наиболее часто встречающихся паролей, рассчитать их хеши и сравнить полученные результаты с хешами из скомпрометированной базы данных. Производительность современных компьютеров позволяет злоумышленникам вычислять миллиарды и даже триллионы хешей в секунду, поэтому даже использование т.н. «соли» — случайного числа, которое добавляется к паролю для изменения его хеша, не гарантирует безопасности. Учитывая, что злоумышленник никак не ограничен по времени взлома и при необходимости может потратить дни и даже месяцы на взлом определённого пользователя, требования к сложности паролей здесь должны быть выше [5–7].

Цель исследования заключается в повышении надёжности паролей пользователей к атакам методом перебора и атакам по словарю с учётом новых рекомендаций к структуре паролей. Проверка возможности атаки на слабые пароли методом перебора и с использованием словаря.

В работе предложены два метода генерации словаря. Первый метод — с использованием вариаций словарных слов и добавлением к ним чисел и комбинаций. Второй метод — с использованием парольных фраз, составленных из случайных словарных слов с учётом грамматики английского языка.

Проанализирована сложность проведения атаки методом перебора на популярные алгоритмы хеширования с использованием графических ускорителей. Предложены рекомендации по генерации словаря для проведения атаки по словарю (в соответствии с новыми рекомендациями к паролям) и способы защиты паролей от таких атак.

Одной из задач для дальнейшего исследования видится сбор статистики по количеству сервисов и провайдеров, предоставляющих возможность использовать в паролях кириллические символы, пробелы, специальные знаки, а также разрешающие создавать длинные пароли (более 64 символов). Вторая практическая задача — написание программы для выполнения хеширования на графическом процессоре по алгоритмам Argon2 и scrypt.

## СПИСОК ЛИТЕРАТУРЫ

1. Grassi P., Fenton J., Newton E., Perlner R., Regenscheid A., Burr W., Richer J. (2024) Digital Identity Guidelines: Authentication and Lifecycle Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63B-4. <https://doi.org/10.6028/NIST.SP.800-63b>.
2. Yildirim, M., Mackie, I. (2019). Encouraging users to improve password security and memorability. *International Journal of Information Security*. 18(12). DOI: 10.1007/s10207-019-00429-y.
3. Shay R., Komanduri S., Kelley P., Leon P., Mazurek M., Bauer L., Christin N., Cranor L. (2010). Encountering Stronger Password Requirements: User Attitudes and Behaviors. *ACM International Conference Proceeding Series*. SOUPS 2010, Redmond, Washington, USA. DOI: 10.1145/1837110.1837113.
4. Weir M., Aggarwal S., Collins M., Stern H. (2010) Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords. *Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS '10*, (ACM, New York, NY, USA), pp 162–175. <https://doi.org/10.1145/1866307.1866327>.
5. Komanduri S., Shay R., Kelley P., Mazurek M., Bauer L., Christin N., Cranor L., Egelman S. (2011). Of passwords and people: Measuring the effect of password-composition policies. *Proceedings of the International Conference on Human Factors in Computing Systems, CHI 2011*, Vancouver, BC, Canada, May 7-12, 2011. DOI: 10.1145/1978942.1979321.
6. Neskey C. Are Your Passwords in the Green? The 2025 Hive Systems Password Table. URL: <https://www.hivesystems.com/blog/are-your-passwords-in-the-green>.
7. Woods N., Siponen M. (2019). Improving Password Memorability, While Not Inconveniencing the User. *International Journal of Human-Computer Studies*. 128. DOI: 10.1016/j.ijhcs.2019.02.003.

УДК 004.08

**РАСПОЗНОВАНИЕ ПОТЕНЦИАЛЬНО ОПАСНЫХ ПРЕДМЕТОВ В РЕАЛЬНОМ ВРЕМЕНИ****Головкин Матвей Максимович**

Санкт-Петербургский государственный университет аэрокосмического приборостроения

Большая Морская ул., 67, Санкт-Петербург, 190121, Россия

e-mail: matvey.golovkin@mail.ru

**Аннотация.** Рассматривается задача распознавания потенциально опасных предметов в реальном масштабе времени. Задача решается с применением нейронной сети YOLOv8, одной из последних разработок в семействе YOLO. Особое внимание уделено созданию кастомного датасета, источниками наполнения которого стали кадры из фильмов и сериалов, игровой контент и открытые источники. Для повышения точности модели в датасет включены изображения предметов, визуально схожих с опасными предметами, но не являющихся ими, что позволило снизить процент ложных срабатываний.

**Ключевые слова:** распознавание; датасет; глубокое обучение; нейронная сеть YOLOv8; обученная модель.

**REAL-TIME DETECTION OF POTENTIALLY DANGEROUS OBJECTS USING DEEP LEARNING****Golovkin Matvey**

Saint Petersburg State University of Aerospace Instrumentation

67 Bolshaya Morskaya St, St. Petersburg, 190121 Russia

e-mail: matvey.golovkin@mail.ru

**Abstract.** The problem of recognizing potentially dangerous objects in real time is considered. The problem is solved using the YOLOv8 neural network, one of the latest developments in the YOLO family. Particular attention is paid to the creation of a custom dataset, the sources of which were frames from films and TV series, game content and open sources. To improve the accuracy of the model, the dataset includes images of objects that are visually similar to dangerous objects, but are not them, which reduced the percentage of false positives.

**Keywords:** detection; dataset; deep learning; neural network YOLOv8; trained model.

В условиях роста угроз безопасности автоматическое обнаружение потенциально опасных предметов на изображениях и видео становится важной задачей. Компьютерное зрение, основанное на методах машинного обучения, позволяет создавать системы для видеонаблюдения, транспорта и общественных мест, способные своевременно выявлять угрозы [1–3].

Качественный датасет — основа эффективной модели компьютерного зрения. Из-за ограниченного доступа к подходящим открытым данным был создан кастомный датасет [4]. Источники данных включали кадры из фильмов и сериалов — сцены из боевиков обеспечили реалистичные изображения оружия и других объектов в разных условиях освещения и ракурсах; игровой контент. Так из игры «Tom Clancy's Ghost Recon Wildlands» было извлечено около 184 000 изображений и после очистки данных для устранения однотипных объектов осталось разнообразное подмножество; открытые источники. Таким образом, видео и изображения из интернета дополнили датасет, увеличив его разнообразие.

Для повышения точности модели в датасет были включены изображения предметов, визуально схожих с оружием, но не являющихся им, таких как зонтики, игрушечные пистолеты. Это позволило модели научиться отличать потенциально опасные объекты от безопасных, избегая ложных срабатываний. Например, зонтик или пластиковый пистолет не помечаются моделью как угроза, а игнорируются в кадре.

Разметка данных включала определение координат ограничивающих рамок и классификацию объектов. Для масштабирования использовался подход semi-supervised learning с псевдоразметкой, состоящий из этапов обучения, автоматической псевдоразметки неразмеченных данных с помощью обученной модели и ручной проверки, и корректировки аннотаций для повышения качества. Обучение выполнялось на 2000 вручную размеченных изображений для создания начальной модели.

Для задачи детекции выбрана модель YOLOv8 (You Only Look Once) — архитектура нейронной сети, разработанная для быстрого и точного обнаружения объектов в реальном времени. YOLOv8 обрабатывает изображение за один проход, предсказывая координаты рамок, классы объектов и оценки достоверности [5, 6].

YOLOv8 использует anchor-free подход — метод обнаружения объектов, при котором отсутствуют предопределённые рамки, что упрощает обучение и повышает гибкость при работе с разнообразными объектами [7].

Обучение проводилось на итоговом датасете с использованием стохастического градиентного спуска и адаптивной скорости обучения. Для повышения обобщающей способности применялись аугментации данных: повороты, изменения яркости и шум. Использование предварительно обученной модели (transfer learning) ускорило процесс и улучшило точность. Модель показала высокую эффективность на тестовых данных, успешно обнаруживая объекты в реальном времени при изменении освещения, углов обзора и масштаба.

Для качественного обучения и проверки работы необходимо разделить все данные на 3 части: train — обучающие данные, которые составили 70%, test — тестовые данные, для проверки во время обучения, которые составили 20 % и valid — проверочные данные, для тестирования модели после обучения, которые составили 10 %. Для обучения понадобилось 500 эпох.

YOLOv8, благодаря своей концепции однопроводной обработки и гибкой архитектуре, показала высокую точность и производительность. Точность (Accuracy) на 12 эпохе достигает 84,7% и далее стабилизируется.

Разработка системы распознавания потенциально опасных предметов требует комплексного подхода к созданию датасета, выбору модели и её обучению. Кастомный датасет, собранный из фильмов, игрового контента и открытых источников, в сочетании с semi-supervised learning обеспечил разнообразие данных.

#### СПИСОК ЛИТЕРАТУРЫ

1. Татарникова Т.М., Бимбетов Ф., Богданов П.Ю. Выявление аномалий сетевого трафика методом глубокого обучения. // Известия СПбГЭТУ ЛЭТИ. 2021. № 4. С. 36-41.
2. Татарникова Т.М., Богданов П.Ю. Обнаружение атак в сетях интернета вещей методами машинного обучения // Информационно-управляющие системы. 2021. № 6 (115). С. 42-52.
3. Sovetov B.Y., Tatarnikova T.M., Cehanovsky V.V. Detection system for threats of the presence of hazardous substance in the environment // Proceedings of 2019 22nd International Conference on Soft Computing and Measurements, SCM 2019. 22. 2019. С. 121-124.
4. Татарникова Т.М., Журавлев А.М. Нейросетевой метод обнаружения вредоносных программ на платформе Android // Программные продукты и системы. 2018. № 3. С. 543-547.
5. YOLOv8 // URL: <https://docs.ultralytics.com/ru/models/yolov8/> (дата обращения 05.05.2025).
6. YOLOv8 Architecture: A Deep Dive into its Architecture // URL: <https://yolov8.org/yolov8-architecture/> (дата обращения 05.05.2025).
7. Татарникова Т.М., Пойманова Е.Д., Богданов П.Ю., Краева Е.В., Вережкин С.А. Программные среды для изучения основ нейронных сетей // Программные продукты и системы. 2021. № 1. С. 145-150.

УДК 004.056

### ЦИФРОВОЙ ДВОЙНИК КАК ИСТОЧНИК РИСКОВ: НЕСОВПАДЕНИЕ С РЕАЛЬНОСТЬЮ И АРХИТЕКТУРА УСТОЙЧИВОСТИ К РАСХОЖДЕНИЯМ

Изотов Даниил Юрьевич, Яровой Роберт Владимирович

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: daniil.izotov.1999@mail.ru, Nadzar@yandex.ru

**Аннотация.** В тезисе рассмотрены причины расхождений, их многоуровневые последствия, подходы к верификации и перспективы создания архитектур, способных удерживать согласованность в условиях неопределённости.

**Ключевые слова:** цифровой двойник; киберфизическая система; рассогласование модели; информационная угроза; устойчивость к несоответствию.

### DIGITAL TWIN AS A SOURCE OF RISKS: DISCREPANCY WITH REALITY AND THE ARCHITECTURE OF RESILIENCE TO DISCREPANCY

Izotov Daniil, Yarovoy Robert

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: daniil.izotov.1999@mail.ru, Nadzar@yandex.ru

**Abstract.** The thesis examines the causes of discrepancies; their multi-level consequences; approaches to verification; and prospects for creating architectures capable of maintaining consistency under conditions of uncertainty.

**Keywords:** digital twin; cyber-physical system; model mismatch; information threat; resilience to mismatch.

Цифровой двойник перестал быть инженерной абстракцией и превратился в активный элемент управления с потенциальной автономией. Чем ближе его ритм к реальному процессу, тем выше риски рассогласования: управляющие импульсы формируются на основе устаревших, зашумлённых или искажённых данных [1].

Формы двойников различаются по степени синхронизации — от периодических до проекционных. Каждая влечёт собственный класс уязвимостей. Источники расхождений включают запаздывание телеметрии, ошибки алгоритмов, асинхронность входных потоков, преднамеренные вмешательства и неполноту модели [2].

По характеру последствий можно выделить четыре типа угроз. Функциональные проявляются в генерации ложных управляющих импульсов. Когнитивные ведут к дезориентации оператора. Информационные связаны с искажением логов и отчётности. Поведенческие выражаются в самоусилении ошибок в самообучающихся системах [3].

Расхождение редко бывает мгновенным — оно накапливается, формируя латентную угрозу, не обнаруживаемую при рутинной диагностике. Основная опасность — в эффекте инерции: модель продолжает действовать по устаревшим представлениям, воспроизводя ошибочные реакции. Подобные случаи зафиксированы в энергетике, транспорте, промышленности и здравоохранении.

Для сдерживания расхождений применяются многомодельные схемы, сопоставляющие данные различных цифровых двойников; сенсоры-резервисты, независимые от модели; адаптивное переобучение при выходе за границы доверия; временные и частотные метрики для оценки стабильности; а также маргинальные фильтры, снижающие значимость нестабильных входов [4].

Цифровой двойник следует воспринимать не как истину, а как гипотезу, требующую постоянной верификации. Развитие идёт в сторону самовосстанавливающихся контуров, когнитивно-интегративных архитектур и нормативного признания двойников как субъектов управления.

Устойчивость — это не совпадение по значениям, а способность своевременно фиксировать, интерпретировать и нейтрализовать расхождение. В этой логике симуляция уступает место метаконтролю: определяющей становится не точность, а зрелость архитектуры.

#### СПИСОК ЛИТЕРАТУРЫ

1. Яровой Р.В., Рябов Г.А., Карганов В.В. Цифровой двойник местности: роль игрового движка в процессе создания, сферы применения двойников // Тенденции развития науки и образования. 2023. № 104-14. С. 152-155.
2. Лычкина Н.Н., Павлов В.В. Концепция цифрового двойника и роль имитационных моделей в архитектуре цифрового двойника // Имитационное моделирование. Теория и практика (ИММОД-2023). Сборник трудов одиннадцатой всероссийской научно-практической конференции по имитационному моделированию и его применению в науке и промышленности. Казань, 2023. С. 139-149.
3. Нистратов А.А. Прогнозирование рисков по цифровому двойнику, сопровождаемому в процессе промышленной эксплуатации объекта // Кибернетика и информационная безопасность «КИБ-2023». Сборник научных трудов Всероссийской научно-технической конференции. Москва, 2023. С. 92-93.
4. Самойлова К.В., Замятина Е.Б. Применение многомодельного подхода к проектированию надежных бизнес-процессов // Имитационное моделирование. Теория и практика (ИММОД-2023). Сборник трудов одиннадцатой всероссийской научно-практической конференции по имитационному моделированию и его применению в науке и промышленности. Казань, 2023. С. 481-490.

УДК 004.738

#### ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ ЦИФРОВЫХ ДВОЙНИКОВ

Краснова Анна Сергеевна<sup>1</sup>, Лямин Александр Сергеевич<sup>1</sup>, Колбанёв Михаил Олегович<sup>2</sup>

<sup>1</sup>Нижегородский государственный инженерно-экономический университет

Октябрьская ул., 22а, Княгинино, 606340, Россия

<sup>2</sup>Санкт-Петербургский государственный экономический университет

Канала Грибоедова наб., 30-32, лит. А, Санкт-Петербург, 191023, Россия

e-mails: shochina96@mail.ru, a.s.lyamin@gmail.com, mokolbanev@mail.ru

**Аннотация.** В работе рассматриваются основные проблемы обеспечения кибербезопасности цифровых двойников, анализируются современные угрозы и предлагаются комплексные подходы к защите.

**Ключевые слова:** цифровой двойник; кибератаки; безопасность; атака; шифрование данных.

#### DIGITAL DOUBLE CYBERSECURITY

Krasnova Anna<sup>1</sup>, Lyamin Alexander<sup>1</sup>, Kolbanev Mikhail<sup>2</sup>

<sup>1</sup>Nizhny Novgorod State University of Engineering and Economics

22a Oktyabrskaya St, Knyaginino, 606340, Russia

<sup>2</sup>St. Petersburg State University of Economics

30-32 Griboedov Channel Emb, St. Petersburg, 191023, Russia

e-mails: shochina96@mail.ru, mokolbanev@mail.ru, mokolbanev@mail.ru

**Abstract.** The paper discusses the main problems of ensuring the cybersecurity of digital twins, analyzes modern threats, and proposes comprehensive approaches to protection.

**Keywords:** digital twin; cyberattacks; security; attack; data encryption.

Современные информационно-коммуникационные услуги охватывают почти все виды жизнедеятельности человека: быт, работу, развлечения, медицину, образование, торговлю и т.д. Основным направлением в развитии информационного сервиса остается расширение перечня услуг и повышение их качества [1]. Современная промышленность так же переживает изменение существующих бизнес-процессов благодаря цифровым технологиям. Производство переходит к интеллектуальному производству, где роль киберфизических систем и цифровых двойников занимают центральное место. Интеллектуальное производство благодаря данным концепциям (киберфизическим системам и цифровым двойникам) контролирует состояние производства в режиме реального времени на протяжении всего жизненного цикла продукта, тем самым в реальном времени они могут: получать информацию об объектах, определять изменение характеристик, делать умозаключение в рамках ранее установленных правил, принимать решения на основе полученной информации и выдать определенные команды.

Актуальность темы обусловлена стремительным ростом внедрения цифровых двойников в важнейшие отрасли, такие как промышленность, энергетика, транспорт и многие другие. Центры обработки данных (ЦОД) объединяющие физический и цифровой миры, создают новые векторы киберугроз при нарушении безопасности ЦОД могут приводить как к утечки данных, так и к физическому ущербу.

Некоторые особенности архитектуры цифровых двойников, а именно:

- многоуровневая структура (датчики, шлюзы, облачные платформы, пользовательские интерфейсы);
- постоянный обмен данными в режиме реального времени;
- зависимость от точности и целостности данных могут стать источником уязвимостей.

Цифровые опасность и безопасность. Построение моделей опасностей предполагает выбор целей и критериев, которые легли бы в основу рациональных решений в области обеспечения безопасности [2].



Основными угрозами и направления атак могут быть подделка или замена данных с датчиков, внедрение вредоносных алгоритмов, DoS/DDoS атаки на платформу ЦОД, утечка конфиденциальности данных.

Анализируя современные подходы и технологии защиты цифровых двойников можно выделить следующие направления для осуществления комплексной безопасности цифровых двойников [3]:

1. Принцип нулевого доверия включающий в себя аутентификацию и авторизацию на каждом этапе взаимодействия.

2. Шифрование данных и использование доверенных вычислений.

3. Цифровые подписи и блокчейн.

4. Система обнаружения аномалий на основе искусственного интеллекта.

5. Сегментация сети и микросегментация.

5. Управление жизненным циклом безопасности.

Безопасность цифровых двойников должна рассматриваться как неотъемлемая часть их архитектуры, а не как дополнительный модуль, тем самым повысив устойчивость к кибератакам, снизит стоимость и сложность защиты, обеспечит гарантию целостности и достоверности модели, обеспечит гибкость и масштабируемость.

#### СПИСОК ЛИТЕРАТУРЫ

1. Микадзе С.Ю., Колбанёв М.О., Татарникова Т.М. Модель информационного взаимодействия для предприятий сервиса // Приборостроение. 2014. №9.
2. Диалектика познания и элиминации «цифровой опасности» когнитивных технологий / М. О. Колбанев, И. Ф. Кефели, К. И. Кефели, А. А. Шамин // Региональная информатика и информационная безопасность : Сборник трудов Санкт-Петербургской международной конференции и Санкт-Петербургской межрегиональной конференции, Санкт-Петербург, 23–25 октября 2024 года. СПб.: СПОИСУ, 2024. С. 176-179.
3. Курганова Н. В., Филин М. А., Черняев Д. С., Шаклеин А. Г., Намиот Д. Е. Внедрение цифровых двойников как одно из ключевых направлений цифровизации производства // International Journal of Open Information Technologies. 2019. №5. URL: <https://cyberleninka.ru/article/n/vnedrenie-tsifrovyyh-dvoynikov-kak-odno-iz-klyuchevykh-napravleniy-tsifrovizatsii-proizvodstva> (дата обращения: 21.08.2025).

УДК 004.056

#### МЕТОДИКА АВТОМАТИЗАЦИИ РАЗРАБОТКИ ПРАВИЛ ОБНАРУЖЕНИЯ АТАК В SIEM

Малахов Максим Юрьевич<sup>1</sup>, Виткова Лидия Андреевна<sup>2</sup>, Нашивочников Николай Васильевич<sup>3</sup>

<sup>1</sup> Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

<sup>2</sup> СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия

<sup>3</sup>ООО «Газинформсервис»

Кронштадтская, 10, Санкт-Петербург, 198096, Россия

e-mails: maksim\_malahov25@mail.ru, vitkova@comsec.spb.ru, cto@gaz-is.ru

**Аннотация.** Безопасность данных внутри корпоративной сети на современном этапе развития информационных систем является критически важным элементом общей эффективности функционирования организации. Для защиты информации специалистами на протяжении многих лет разрабатывались и интегрировались разнообразные системы мониторинга и отражения атак злоумышленников. Примером такой системы может послужить SIEM, стабильность функционирования которой напрямую зависит от качества разработанного контента обнаружения. Автоматизация и оптимизация процесса создания контента, представленного корреляционными правилами позволяет значительно увеличить область охвата источников данных, при этом сокращая затраты времени. Это, безусловно, позитивно сказывается на уровне защиты конфиденциальной информации от несанкционированного доступа. В настоящей статье рассматриваются подходы к автоматизации разработки правил корреляции, а также анализируются их достоинства и недостатки.

**Ключевые слова:** системы мониторинга; правила корреляции; SIEM; автоматизация; информационная безопасность; искусственный интеллект.

#### METHODOLOGY FOR AUTOMATING THE DEVELOPMENT OF ATTACK DETECTION RULES IN SIEM

Malakhov Maksim <sup>1</sup>, Vitkova Lidia <sup>2</sup>, Nashivochnikov Nikolay <sup>3</sup>

<sup>1</sup>The Bonch-Bruevich Saint Petersburg State University of Telecommunications  
22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia

<sup>2</sup>St. Petersburg Federal Research Center of the Russian Academy of Sciences  
39 14th Line VO, St. Petersburg, 199178, Russia

<sup>3</sup>Limited Liability Company «Gazinformservice»  
10 Kronshtadtskaya, St. Petersburg, 198096, Russia

e-mails: maksim\_malahov25@mail.ru, vitkova@comsec.spb.ru, cto@gaz-is.ru

**Abstract.** Data security within a corporate network is a critically important element of an organization's overall operational efficiency at the current stage of information systems development. Over the years, experts have developed and integrated various monitoring and attack defense systems to protect information. One example of such a system is SIEM, the stability of which directly depends on the quality of the detection content developed. Automating and

optimizing the creation of content, represented by correlation rules, can significantly expand the coverage of data sources while reducing time costs. This undoubtedly has a positive impact on the level of protection of confidential information against unauthorized access. This article explores approaches to automating the development of correlation rules and analyzes their advantages and disadvantages.

**Key words:** monitoring systems; correlation rules; SIEM; automation, information security; artificial intelligence.

На сегодняшний день обеспечение информационной безопасности внутри корпоративной сети выступает критически значимым фактором для стабильного функционирования организации. В условиях динамично растущих киберугроз первостепенное значение приобретает задача защиты персональной, рабочей и коммерческой информации, гарантируя ее конфиденциальность от несанкционированного доступа. SIEM-системы, безусловно, представляют собой перспективное решение для преодоления этих вызовов, поскольку имеется возможность в расширении базы отслеживания нелегитимных действий в соответствии с новыми тенденциями их исполнения, а также появлением новых тактик и техник, к которым прибегают злоумышленники [1, 2].

Центральным звеном работы каждой из систем противодействия угрозам информационной безопасности является контент обнаружения — технология, основанная на алгоритмах глубокого обучения, позволяющая фиксировать компрометирующие действия стороннего пользователя, используя различные индикаторы нелегитимной активности.

Одной из ключевых трудностей при работе с обнаружением контента в системах SIEM является недостаточная скорость создания новых правил [3], а также сложность в исследовании новых векторов атак. Ведь, если контент для детектирования отсутствует, организация остаётся беззащитной перед новыми способами взлома. Из этого логично вытекает необходимость автоматизировать процессы, связанные с разработкой контента обнаружения.

Цель доклада — разработка методики автоматизации разработки контента обнаружения с помощью практического тестирования различных подходов формирования корреляционных правил.

Разработка контента происходит с помощью актуальных кейсов информационной безопасности, одними из основных банков для написания правил служат зарубежная матрица MITRE ATT&CK, отечественная БДУ ФСТЭК и репозиторий правил Sigma, на основании последней в рамках исследования проводилось тестирование по конвертации выборки правил с помощью утилит и искусственного интеллекта.

На первом этапе эксперимента используется ручной подход к написанию правил — для разработки правил корреляции не используются средства автоматизации, сами правила формируются аналитиком систем мониторинга безопасности.

Основным фактором оценки эффективности подхода является затраченное время, поскольку написание происходит нераспределенным методом. Аналитиком прописывается маппинг корреляционного события в соответствии инструкции 'on', добавляются уникальные поля корреляции, содержащие информацию о критичности события, а также категоризация — двухуровневый метод разбиения, дающий краткую классификацию каждого формируемого корреляционного события.

На втором этапе эксперимента применяется автоматизированный подход с использованием конвертера — для разработки правила используется конвертер правил корреляции, отобранных в открытом репозитории универсальных правил Sigma. Промежуточным результатом методики является уменьшение времени написания правил со среднего значения ручного метода в 38,7 минут до 35 минут, что свидетельствует о положительной динамике процесса автоматизации разработки правил и необходимости проведения заключительного этапа эксперимента.

Заключительный этап эксперимента включает в себя использование автоматизированного подхода с использованием языковой модели — для разработки правил используется заранее сформированный промпт-запрос с изложением приблизительного объема маппинга и примерами конвертации правил, не участвующих в реализации методики.

Таким образом, реализуется Chain-of-Thought prompting — методика обучения языковой модели, побуждающая искусственный интеллект формировать результат с предоставлением пошагового объяснения мыслительного процесса при решении поставленной задачи. Результатом методики является уменьшение времени написания правил со среднего значения ручного метода в 38,7 минут до 21 минуты, что позволяет в потенциале оптимизировать процесс написания правил на 45 процентов.

Полученные результаты подчеркивают возможность интеграции методики разработки корреляционных правил в процесс написания контента обнаружения, поскольку применение средств автоматизации задает положительную тенденцию в сокращении затрачиваемого времени на формирование корреляционных правил.

#### СПИСОК ЛИТЕРАТУРЫ

1. Kotenko I., Gaifulina D., Zelichenok I. Systematic Literature Review of Security Event Correlation Methods // IEEE Access, 2022. С. 4-7.
2. Котенко И.В., Ушаков И.А., Пелёвин Д.В., Преображенский А.И., Овраменко А.Ю. Выявление инсайдеров в корпоративной сети: подход на базе UBA И UEBA // Защита информации. Инсайд. 2019. № 5 (89). С. 26-35.
3. Что такое Detection Engineering и с чем его едят // ptresearch URL: <https://ptresearch.media/articles/chto-takoe-detection-engineering-i-s-chem-ego-edyat> (дата обращения: 10.08.2025).

УДК 004.622

**ОБНАРУЖЕНИЕ АТАК И ВИРУСОВ НА ОСНОВЕ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ****Пойманова Екатерина Дмитриевна**

Санкт-Петербургский государственный университет аэрокосмического приборостроения

Большая Морская ул., 67, Санкт-Петербург, 190121, Россия

e-mail: e.d.poymanova@gmail.com

**Аннотация.** Обсуждается задача применения искусственных нейронных сетей при построении систем обнаружения атак и антивирусных систем, что обусловлено необходимостью раннего предупреждения о наличии компьютерных атаках в сетевом трафике и несостоятельностью сигнатурных методов обнаружить сложный класс АРТ-атак и новых еще неизвестных атак класса Zero Day, а также модифицируемых компьютерных вирусов. Приводится разработанный алгоритм и описание программной реализации системы обнаружения атак на основе искусственной нейронной сети. Предложенный метод является сопутствующим к статистическим методам, на которых построены современные системы обнаружения атак и антивирусные системы.

**Ключевые слова:** система обнаружения атак; нейронная сеть; оптимальная архитектура нейронной сети; обучающая выборка; библиотеки для обучения; эффективность обнаружения атак.

**ATTACK AND VIRUS DETECTION BASED ON ARTIFICIAL NEURAL NETWORKS****Poymanova Ekaterina**

Saint Petersburg State University of Aerospace Instrumentation

67 Bolshaya Morskaya St, St. Petersburg, 190121 Russia

e-mail: e.d.poymanova@gmail.com

**Abstract.** The problem of using artificial neural networks in building attack detection systems and antivirus systems is discussed, which is caused by the need for early warning about the presence of computer attacks in network traffic and the failure of signature methods to detect a complex class of APT attacks and new yet unknown Zero Day attacks, as well as modified computer viruses. The developed algorithm and description of the software implementation of an attack detection system based on an artificial neural network are presented. The proposed method is an accompanying one to statistical methods, on which modern attack detection systems and antivirus systems are built.

**Keywords:** intrusion detection system; neural network; optimal neural network architecture; training set; libraries for training; intrusion detection efficiency.

В связи с увеличением вычислительных возможностей программно-аппаратных комплексов, в том числе в результате использования графических процессоров и распределенных архитектур вычислительных систем, стало доступным широкое применение искусственных нейронных сетей (ИНС), в том числе при построении систем обнаружения атак (СОА) и антивирусных систем (АВС) [1]. Обращение к активному использованию ИНС обусловлено необходимостью раннего предупреждения о наличии компьютерных атаках в сетевом трафике и несостоятельностью сигнатурных методов обнаружить сложный класс АРТ-атак (advanced persistent threat) и новых еще неизвестных атак класса Zero Day, а также модифицируемых компьютерных вирусов [2]. Методы, основанные на применении ИНС, являются сопутствующими к статистическим методам, на которых основаны СОА и АВС.

В работе приводится разработанный алгоритм и описание программной реализации СОА на основе ИНС, целью которой является повышение эффективности функционирования СОА.

Построение СОА на основе ИНС подразумевает решение ряда важных задач, таких как формирование исходного набора данных для обучения (датасета), выбор типа нейронной сети, ее гиперпараметров и тестирования ИНС. Для обучения ИНС используются датасеты — выборки с размеченными классами атак. Такие атаки как переполнение буфера (buffer overflow), неправильная аутентификация (brute force), SQL-инъекция, DoS-атака, XSS-атака являются наиболее распространенными. Самые популярные датасеты — NSL-KDD [3] и KYOTO 2006+ [4]. Первый датасет создан искусственно в виртуальных сетях, второй — основан на реальном сетевом трафике. Эти и другие «датасеты» также собраны в [5].

Датасеты имеют определенную структуру, которая формируется из исходного сетевого трафика, проходящего предобработку. Предлагается использовать в качестве исходной выборки «чистый» сетевой трафик, без преобразования исходных данных в другой формат. Это позволит сократить время преобразования данных в специальный формат, особенно это актуально для высокоскоростного сетевого трафика. Следовательно, используемые данные должны быть представлены в виде рсар-файла(-ов). Соответственно, предполагается достигнуть точность обнаружения атак — 85%, что является нижней границей достигнутых результатов других исследований, но для размеченных датасетов (от 85% до 99%).

Процесс функционирования СОА начинается с формирования обучающей выборки ИНС. Входящий сетевой трафик на основе списка выбранных атак формируется в датасет, который сохраняется в директорию. Датасет запускает два параллельных процесса: поиск оптимальной модели ИНС с учетом запрашиваемых гиперпараметров ИНС и нормализацию данных обучающей выборки. Далее, на основе специальных библиотек и полученного набора оптимальных гиперпараметров происходит обучение ИНС. И уже обученная модель готова анализировать другие предварительно нормализованные данные, выдавая на выходе некоторые предсказания. Используя стандартные общеизвестные параметры протоколов, можно откорректировать полученные предсказания.

Обучающую выборку можно сформировать и самостоятельно, например с помощью программы Snort [6]. Сетевой пакет, попав в Snort, последовательно проходит через декодеры, задача которых состоит в том, чтобы извлечь данные сетевого и транспортного уровней. Далее эти данные преобразуются в специальный формат, после чего к ним применяются правила. В правилах содержится информация о трафике, искомой сигнатуре, описании угрозы и как необходимо реагировать на нее.

Сформированную выборку данных необходимо разделить на два множества: обучающее и тестовое. Для каждого множества создана таблица с метками pcap-файлов, в данной работе — csv-файлы.

Для уточнения архитектуры ИНС используется библиотека Keras Tuner — определение гиперпараметров ИНС, в которые входят, например, количество слоев, их размеры, функции активации и пр. [7].

В качестве языка программирования выбран Python, имеющий библиотеки для работы с большими данными: dpkt, numpy, tqdm, csv и argparse.

Входные данные представляют собой множество pcap-файлов, расположенных в одном каталоге. Файлы содержат сетевой трафик с классифицируемыми атаками. Выходной файл представляет собой таблицу в виде csv-файла. Эксперименты проводились в виртуальной машине, запущенной в программном обеспечении для виртуализации VMware со следующими характеристиками: операционная система — Linux Ubuntu, разрядность процессора — 64 бита, оперативная память — 8 Гб, количество процессоров — 2, количество ядер — 8.

Первая серия экспериментов проводилась для выбора архитектуры ИНС. Процедура поиска оптимальной модели была запущена несколько раз — для разного количества скрытых слоев. Для каждой итерации использовался один и тот же датасет.

Этап обучения ИНС схож с этапом поиска ее оптимальной архитектуры. Для этого использовались те же обучающие и тренировочные данные. Основное отличие заключается в том, что на выходе процедуры обучения формируется модель ИНС, сохраняемая в файл, которую в дальнейшем можно использовать для анализа сетевого трафика. Полученные оптимальные архитектуры ИНС сохраняются в отдельных файлах. Оценка эффективности СОА производилась по двум параметрам: доли обнаруженных атак и доли ложных срабатываний. В эксперименте используется примерно 5200 сетевых пакетов, из них примерно 3500 пакетов содержат угрозу.

Для выявления неизвестных атак проведен отдельный эксперимент, при этом была заново обучена ИНС на данных, в которых фигурировали только 4 атаки, а оставшиеся данные использовались для тестирования обнаружения неизвестной атаки «brute force».

Отличие данного исследования от других в том, что использован «чистый» сетевой трафик. И полученная в экспериментах точность в 94-98% оказалась выше ожидаемой и сравнима с результатами других исследований, где используются готовые «датасеты» с искусственными данными.

#### СПИСОК ЛИТЕРАТУРЫ

1. Tsai C.F., Hsub Y.F., Linc C.Y., Lin W.Y. Intrusion detection by machine learning: A review // Expert Systems with Applications. 2009. vol. 36. Issue 10. P. 11994–12000.
2. Сафронова Е. О., Жук Г. А. Применение искусственных нейронных сетей для прогнозирования DoS атак // Молодой ученый. 2019. №23. С. 27-30
3. Ландшафт угроз для систем промышленной автоматизации [Электронный ресурс] // Kaspersky Lab ICS CERT. URL: [https://icscert.kaspersky.ru/reports/2018/03/26/threat-landscape-for-industrial-automationsystems-in-h2-2017/#\\_Toc508825260](https://icscert.kaspersky.ru/reports/2018/03/26/threat-landscape-for-industrial-automationsystems-in-h2-2017/#_Toc508825260) (дата обращения: 20.06.2023).
4. NSL-KDD dataset [Electronic resource] // University of New Brunswick. URL: <https://www.unb.ca/cic/datasets/nsf.html> (дата обращения: 20.06.2023).
5. Traffic Data from Kyoto University's Honeypots [Electronic resource] // URL: [http://www.takakura.com/Kyoto\\_data/](http://www.takakura.com/Kyoto_data/) (дата обращения: 20.06.2023).
6. Датасеты по информационной безопасности для машинного обучения [Электронный ресурс] // SecurityLab.ru by Positive Technologies. URL: [https://www.securitylab.ru/blog/personal/Business\\_without\\_danger/345789.php](https://www.securitylab.ru/blog/personal/Business_without_danger/345789.php) (дата обращения: 20.06.2023).
7. Бахарева Н.Ф., Тарасов В.Н., Шухман А.Е. Выявление атак в корпоративных сетях с помощью методов машинного обучения // Современные информационные технологии и ИТ-образование. 2018. № 3. С. 626-632.
8. Татарникова Т.М., Бимбетов Ф., Богданов П.Ю. Выявление аномалий сетевого трафика методом глубокого обучения // Известия СПбГЭТУ ЛЭТИ. 2021. № 4. С. 36-41.
9. Анчишкин А.П. Сравнительный анализ современных систем обнаружения вторжений // Colloquium-Journal. 2019. № 26 (50). С. 25-27.
10. Thing, V. IEEE 802.11 Network Anomaly Detection and Attack Classification: A Deep Learning Approach [Text] / V. Thing // 2017 IEEE Wireless Communications and Networking Conference (WCNC). San Francisco, CA. 2017. P. 1-6.
11. Татарникова Т.М., Богданов П.Ю. Обнаружение атак в сетях интернета вещей методами машинного обучения // Информационно-управляющие системы. 2021. № 6 (115). С. 42-52.

УДК 519.85

#### ОПТИМИЗАЦИЯ НЕЙРОННЫХ СЕТЕЙ ЧЕРЕЗ ПОЛУСТРУКТУРИРОВАННУЮ РАЗРЕЖЕННОСТЬ АКТИВАЦИЙ

Раскопина Анастасия Сергеевна

Санкт-Петербургский государственный университет аэрокосмического приборостроения

Большая Морская ул., 67, Санкт-Петербург, 190121, Россия

e-mail: raskopina.anastasia@yandex.ru

**Аннотация.** Автоматизация анализа рукописных документов решается с применением технологий обработки изображений. Рукописные тексты представляют собой сложный объект для извлечения информации из-за разнообразия стилей письма, различных уровней чёткости и наличия шумов. Шум может проявляться в виде дефектов, размытости или искажений. В статье рассмотрено несколько подходов по удалению клетки на листе бумаги с использованием библиотеки OpenCV языка Python.

**Ключевые слова:** рукописный документ; извлечение информации; шумы; обработка изображений; компьютерное зрение.

## OPTIMIZATION OF NEURAL NETWORKS THROUGH SEMI-STRUCTURED SPARSITY OF ACTIVATIONS

Raskopina Anastasia

Saint Petersburg State University of Aerospace Instrumentation  
67, Bolshaya Morskaya St, St. Petersburg, 190121 Russia  
e-mail: raskopina.anastasia@yandex.ru

**Abstract.** Automation of handwritten document analysis is solved using image processing technologies. Handwritten texts are a complex object for information extraction due to the variety of writing styles, different levels of clarity and the presence of noise. Noise can manifest itself in the form of defects, blurriness or distortion. The article considers several approaches to removing a cell on a sheet of paper using the OpenCV library of the Python.

**Keywords:** handwritten document; information extraction; noise; image processing; computer vision.

Современные нейронные сети демонстрируют высокую эффективность в решении сложных задач машинного обучения, таких как компьютерное зрение, обработка естественного языка и генерация данных. Однако в последние годы нейронные сети значительно увеличили свою глубину и сложность, что привело к росту вычислительных затрат и потребности в мощном оборудовании. До 2010 года по закону Мура вычислительные ресурсы для обучения моделей удваивались каждые 20 месяцев, но после распространения глубокого обучения возрастание значительно ускорилося и вычислительные ресурсы начали удваиваться примерно раз в 6 месяцев. В том числе, большие компании начали финансировать проекты по разработке крупномасштабных моделей машинного обучения и тогда требования к вычислительным ресурсам стали превышать предыдущие от 10 до 100 раз. Все это привело к тому, что обучение и инференс стали медленными и дорогостоящими, поскольку высокая вычислительная сложность требует значительных аппаратных мощностей. Это ограничивает применение сложных моделей на устройствах с ограниченными ресурсами или их нехваткой, например, на мобильных телефонах и устройствах IoT.

В настоящее время специалисты все чаще задаются вопросом оптимизации нейросетей для решения этих проблем, стремясь при этом не терять точность моделей. Одним из эффективных методов, существующих на данный момент, является разреживание активаций. Этот метод удаляет наименее значимые элементы в выходах нейронов, что позволяет уменьшить количество вычислений и объем передаваемых данных, что особенно важно для устройств с ограниченными ресурсами.

Существует несколько видов разреживания. В данной статье рассматриваются основные виды разреживания, с особым акцентом на полуструктурированную разреженность активаций, потому что данный подход считается самым гибким и сбалансированным, позволяя значительно снизить затраты на вычисления без существенного падения точности модели.

В данной статье подробно рассмотрим методы внедрения этого подхода, оценим его влияние на производительность моделей и представим экспериментальные результаты [1–3].

Работа метода разреживания активаций основана на сокращении количества активных элементов в выходных тензорах слоев нейросети. Как уже было сказано ранее, данный метод позволяет снизить потребление памяти и ускорить инференс. Методы разреживания активаций различаются по способу зануления активаций:

1. Неструктурированное разреживание зануляет отдельные элементы тензоров, основываясь на их важности. Такой подход является очень гибким, так как позволяет удалять любые незначимые элементы вне зависимости от их расположения в тензоре. Однако данный вариант сложно реализовать на аппаратном уровне, поскольку нерегулярное распределение нулей препятствует оптимизированному выполнению операций на графических процессорах (GPU) и тензорных процессорах (TPU). В конечном итоге такая гибкость не всегда приводит к значительному ускорению вычислений, поскольку снижается эффективность пакетной обработки.

2. Структурированное разреживание, как видно из названия, является полной противоположностью неструктурированного метода. В этом случае зануление происходит на уровне более крупных единиц данных, таких как каналы, фильтры, нейроны и даже целые слои. Данный метод может значительно уменьшить размер модели и ускорить инференс, а также улучшает совместимость с аппаратными ускорителями, поскольку зануление носит регулярный характер. Однако существенный минус этого метода — возможное значительное снижение точности. Кроме того, требуется тщательная настройка и отбор элементов для зануления, чтобы минимизировать потери качества предсказаний.

3. Полуструктурированное разреживание является компромиссом между двумя предыдущими методами, учитывая их преимущества и недостатки. В данном подходе зануление происходит не на уровне отдельных элементов (как в неструктурированном методе) и не на уровне целых фильтров или каналов (как в структурированном методе), а на уровне небольших групп или блоков элементов. Этот метод требует дополнительного контроля, так как разбиение тензоров на блоки может потребовать дополнительного анализа и экспериментов. Однако его главное преимущество заключается в том, что он удобен для аппаратной реализации, обеспечивает значительное сокращение вычислительных затрат и при этом минимально влияет на точность модели.

Каждый из представленных методов имеет свои преимущества и ограничения. Выбор подходящего метода зависит от конкретной задачи, но полуструктурированное разреживание является оптимальным вариантом, потому что он помогает оптимизировать нейросеть и не терять значительно точность модели [4, 5].

Для внедрения полуструктурированной разреженности применяются различные подходы, позволяющие эффективно уменьшить вычислительные затраты без значительного падения точности.

Один из основных методов — обучение с регуляризацией, например, с использованием L1-регуляризации. Этот метод добавляет к функции потерь штраф за ненулевые активации, тем самым способствуя занулению наименее значимых элементов.

Еще один эффективный подход является квантование. Он снижает разрядность чисел с плавающей запятой, например, переход от 32-битных значений к 8-битным, что значительно уменьшает объем вычислений и потребление памяти. Также существует динамическое разреживание, при котором нейроны отключаются во время инференса в зависимости от входных данных. Такой метод позволяет адаптировать вычислительные затраты к конкретной задаче и текущей нагрузке.

Эти методы могут комбинироваться и применяться одновременно без критического падения точности, однако их настройка требует тщательного подбора гиперпараметров. При неправильной конфигурации разреживание может привести к существенному ухудшению качества модели.

Проведенный эксперимент на стандартном датасете ImageNet при использовании архитектуры ResNet-50 показал, что полуструктурированное разреживание позволяет сократить время инференса почти в 1.7 раза, сохраняя точность на уровне оригинальной модели.

Полуструктурированная разреженность активаций является перспективным методом оптимизации нейронных сетей, который позволяет значительно ускорить их работу без критической потери качества. Данный подход особенно актуален для мобильных и встраиваемых систем, где ресурсы ограничены, а также для облачных сервисов, где важно снижать вычислительные затраты.

Применение полуструктурированного разреживания способствует разработке более энергоэффективных и быстрых моделей, что делает его ценным инструментом в современной индустрии искусственного интеллекта.

В ходе эксперимента использование данного метода позволило сократить время инференса почти в 1.7 раза при минимальных потерях точности модели. Это подтверждает его эффективность и практическую применимость. Конечно, внедрение такого подхода в реальные приложения требует адаптации к конкретным архитектурам и задачам, но уже сейчас он демонстрирует значительные преимущества.

#### СПИСОК ЛИТЕРАТУРЫ

1. Sajid, A. Fixed point optimization of deep convolutional neural networks for object recognition / A. Sajid, H. Kyuyeon, S. Wonyong // *Speech and Signal Processing (ICASSP)*, 2015 IEEE International Conference. 2015. P. 1131–1135.
2. Matthieu, C. Binary connect: Training deep neural networks with binary weights during propagations / C. Matthieu, B. Yoshua, D. Jean-Pierre // *In NeurIPS — Advances in Neural Information Processing Systems*. 2015. P. 3123–3131.
3. Han, S. Deep compression: Compressing deep neural networks with pruning, trained quantization and Huffman coding / S. Han, H. Mao, W. J. Dally, arXiv preprint arXiv:1510.00149.
4. He, Y. Channel pruning for accelerating very deep neural networks / Y. He, X. Zhang, J. Sun // *International Conference on Computer Vision*. 2017. C. 1389–1397.
5. Татарникова, Т.М., Пойманова, Е.Д., Богданов, П.Ю., Краева, Е.В., Вережкин, С.А. Программные среды для изучения основ нейронных сетей / Т. М. Татарникова, Е. Д. Пойманова, П. Ю. Богданов, Е. В. Краева, С. А. Вережкин // *Программные продукты и системы*. 2021. № 1. С. 145–150.

УДК 004.62

#### МОДЕЛИ МИГРАЦИИ В СИСТЕМАХ ХРАНЕНИЯ ДАННЫХ

**Решетников Дмитрий Сергеевич**

Санкт-Петербургский государственный университет аэрокосмического приборостроения

Большая Морская ул., 67, Санкт-Петербург, 190121, Россия

e-mail: rdsrdsrds2001@gmail.com

**Аннотация.** Рассматривается оптимизация ETL-процессов репликации данных из Apache Hive в Clickhouse в условиях роста объемов данных и ухода европейских сервисов с российского рынка. Предлагается новый подход, основанный на использовании Apache Airflow, PySpark и Jupyter Notebook, который обеспечивает более безопасную, быструю и экономически эффективную репликацию данных.

**Ключевые слова:** хранилище данных; производительность; миграция данных; репликация данных; ETL-процесс; системы управления данными с открытым исходным кодом.

#### MIGRATION MODELS IN DATA STORAGE SYSTEMS

**Reshetnikov Dmitry**

Saint Petersburg State University of Aerospace Instrumentation

67, Bolshaya Morskaya St, St. Petersburg, 190121 Russia

e-mail: rdsrdsrds2001@gmail.com

**Abstract.** The article considers the optimization of ETL processes for data replication from Apache Hive to Clickhouse in the context of growing data volumes and the departure of European services from the Russian market. A

new approach based on the use of Apache Airflow, PySpark and Jupyter Notebook is proposed, which provides more secure, fast and cost-effective data replication.

**Keywords:** data warehouse; performance; data migration; data replication; ETL process; open source; data management systems.

В условиях стремительного роста объемов данных, многие организации сталкиваются с необходимостью эффективной обработки и анализа информации. Одним из ключевых подготовительных этапов, способствующих решению таких задач являются ETL-процессы (ETL — Extract, Transform, Load, что соответствует последовательным этапам процесса — Извлечение, Преобразование и Загрузка) [1].

Извлечение (Extract) — данные извлекаются из различных исходных систем, таких как базы данных, файлы, облачные сервисы и другие.

Преобразование (Transform) — полученные данные проходят обработку, которая включает в себя очистку, преобразование в единый формат, удаление дубликатов, заполнение пропусков, агрегацию и другие операции.

Загрузка (Load) — преобразованные данные загружаются в целевую систему, например, хранилище данных, для дальнейшего анализа и использования.

В итоге, ETL-процессы позволяют:

- интегрировать данные из различных источников в единую систему;
- обеспечить качество и целостность данных, необходимых для аналитики;
- создать централизованное хранилище данных для поддержки принятия бизнес-решений;
- автоматизировать процесс подготовки данных для различных целей.

Работа посвящена исследованию процессов миграции больших данных, с акцентом на ETL-репликацию данных из Apache Hive — системы управления реляционными базами данных с открытым исходным кодом в Clickhouse — систему управления колоночными базами данных с открытым исходным кодом. Целью работы является разработка альтернативного решения для репликации данных, построенного на открытом исходном коде, которое является более эффективным по сравнению с существующими методами

Необходимость репликации данных в колоночную СУБД для дальнейшей работы с витринами данных, объясняется следующими факторами [2, 3]:

- хранение данных по столбцам позволяет увеличивать производительность запросов, например, агрегирование данных выполняется быстрее, поскольку СУБД считывает только требуемые столбцы;
- благодаря хранению однотипных данных в колонках достигается высокая степень сжатия (до 10х по сравнению с реляционной моделью данных), что обеспечивают более экономное использование хранилища;
- колоночные СУБД адаптированы для OLAP-запросов к данным, хранящимся в OLAP-кубах, что позволяет анализировать данные с разных точек зрения.

Существующие ETL-процессы не всегда обеспечивают требуемую производительность и надежность, а также обоснованную стоимость. Кроме того, в последние годы на отечественном рынке наблюдается значительное изменение в организации репликации данных, вызванное уходом европейских сервисов и компаний, что обуславливает поиск новых подходов к обработке больших данных [4–6].

Новый ETL-процесс реализован с использованием:

- Apache Airflow — платформы с открытым исходным кодом для создания, выполнения, мониторинга и оркестровки потоков операций по обработке данных — для управления задачами;
- PySpark — инструмент для обработки больших объемов данных и аналитики, позволяющий разработчикам Python использовать распределенные вычисления фреймворка Spark для эффективной обработки больших наборов данных в кластерах;
- Jupyter Notebook — это интерактивная веб-среда для работы с кодом, данными и визуализациями.

Данный набор инструментов позволяет оптимизировать взаимодействие между системами хранения данных.

Озеро данных представляет собой универсальную платформу для хранения больших объемов данных из различных источников в их исходном виде.

Колоночная СУБД (колоночная база данных) — это тип системы управления базами данных, который хранит данные в виде столбцов, а не строк. Это позволяет значительно повысить эффективность хранения и обработки данных, особенно для аналитических запросов, которые часто требуют агрегации и выборки по большим объемам информации.

Централизованное хранилище предназначено для хранения и управления структурированными и очищенными данными, собранными из разных источников для поддержки конкретной задачи бизнес-анализа и отчетности.

Витрина данных — подмножество (срез) хранилища данных, представляющее собой массив тематической, узконаправленной информации, ориентированной, например, на пользователей одной рабочей группы или подразделения.

Для решения поставленной задачи привлечены следующие инструменты и библиотеки: Apache Airflow, Jupyter Notebook, Apache Hive, Clickhouse, Python и его библиотеки: PySpark — необходима для взаимодействия со Apache Spark, argparse — необходима для того, чтобы передавать данные из конвейера данных в скрипт в Jupyterlab, airflow — необходима для того, чтобы создать конвейер данных в Apache Airflow с необходимыми

параметрами, ipywidgets — необходима для реализации дружественного интерфейса в приложении, чтобы пользователи могли пользоваться данным движком.

По результатам натурного эксперимента можно сделать вывод, что решение, представленное в работе с точки зрения времени выполнения ETL-процесса, занимаемой памяти при репликации и надежности выполнения ETL-процесса является предпочтительнее существующих современных решений: 1) движка HDFS для репликации данных и 2) ClickHouse Driver, Apache Kafka и Apache NiFi — набора инструментов для работы с большими данными: ClickHouse Driver — драйвер для подключения к базе данных ClickHouse, который позволяет передавать данные из Apache Kafka в ClickHouse. Apache Kafka — распределённая система для обработки потоков данных в реальном времени, Apache NiFi — инструмент для автоматизации потоков данных между системами хранения данных. Важно отметить, что чем больше объем данных берется для тестирования, тем предпочтительней выглядит данное решение.

Результаты проведенной работы подчеркивают важность и необходимость оптимизации ETL-процессов в условиях стремительного увеличения объемов данных. Разработка более эффективного подхода к репликации данных из Apache Hive в Clickhouse отвечает современным требованиям бизнеса и открывает новые возможности для повышения производительности систем хранения и обработки информации.

#### СПИСОК ЛИТЕРАТУРЫ

1. Юдин И.А., Решетников Д.С. Создание ETL-движка для репликации данных из Apache Hive в Clickhouse. Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2024. С. 371-37.
2. Пойманова Е.Д., Татарникова Т.М., Краева Е.В. Модель управления хранением трафика данных // Известия высших учебных заведений. Приборостроение. 2021. Т. 64. № 5. С. 370-375.
3. Татарникова Т.М., Архипцев Е.Д. Алгоритм контроллера нечеткой логики для размещения файлов в системе хранения данных // Научно-технический вестник информационных технологий, механики и оптики. 2023. Т. 23. № 6. С. 1171-1177.
4. Chen, S., Wang, Z., Bai, L., Liu, K., Gao, J., Zhao, M., and Mulvenna, M. D.: Large vector spatial data storage and query processing using ClickHouse, Int. Arch. Photogramm. Remote Sens. Spatial Inf. Sci., XLVIII-M-1-2023, 65–72, doi: 10.5194/isprs-archives-XLVIII-M-1-2023-65-2023, 2023.
5. Татарникова Т.М., Пойманова Е.Д. Методика дифференцированного наращивания емкости системы хранения данных с многоуровневой структурой // Научно-технический вестник информационных технологий, механики и оптики. 2020. Т. 20. № 1. С. 66-73.
6. Татарникова Т.М., Архипцев Е.Д., Кармановский Н.С. Определение размера кластера и числа реплик высоконагруженных информационных систем // Известия высших учебных заведений. Приборостроение. 2023. Т. 66. № 8. С. 646-651.

УДК 004.8

#### ГЕНЕРАЦИЯ СИНТЕТИЧЕСКОГО ТРАФИКА ИНТЕРНЕТА ВЕЩЕЙ ПРИ РЕШЕНИИ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Савельева Дарья Дмитриевна

Санкт-Петербургский государственный университет аэрокосмического приборостроения  
Большая Морская ул., 67, Санкт-Петербург, 190121, Россия  
e-mail: savel.dar.23@mail.ru

**Аннотация.** В работе описаны методы получения трафика интернета вещей для выполнения его анализа с целью детектирования аномалий в трафике интернета вещей. Показано, что анализ трафика интернета вещей реализуется с привлечением методов машинного обучения и наличия датасетов. Сбор датасета с оригинальными данными является сложной задачей, которая не гарантирует отсутствие шумов, дисбаланса классов, обеспечение конфиденциальности, что позволяет использовать синтетические наборы данных. В статье представлены модели генерации синтетического трафика, которые изучают лежащие в основе закономерности и распределения оригинальных данных и повторяют характеристики трафика интернета вещей.

**Ключевые слова:** интернет вещей; реальный трафик; синтетический трафик; нейросетевой синтезатор; валидация данных.

#### GENERATION OF SYNTHETIC TRAFFIC OF THE INTERNET OF THINGS IN SOLVING INFORMATION SECURITY PROBLEMS

Savelyeva Daria

Saint Petersburg State University of Aerospace Instrumentation  
67 Bolshaya Morskaya St, St. Petersburg, 190121 Russia  
e-mail: savel.dar.23@mail.ru

**Abstract.** The paper describes methods for obtaining Internet of Things traffic to perform its analysis in order to detect anomalies in Internet of Things traffic. It is shown that Internet of Things traffic analysis is implemented using machine learning methods and the presence of datasets. Collecting a dataset with original data is a complex task that does not guarantee the absence of noise, class imbalance, and confidentiality, which allows the use of synthetic datasets. The article presents synthetic traffic generation models that study the underlying patterns and distributions of original data and replicate the characteristics of Internet of Things traffic.

**Keywords:** internet of things; real traffic; synthetic traffic; neural network synthesizer; data validation.



В последние десятилетия наблюдается значительный рост интереса и практического применения технологии, известной как Интернет вещей (IoT). Технология позволяет интегрировать вычислительные устройств в повседневные объекты, и развивается из теоретической разработки в одну из наиболее развивающихся технологических направлений. В настоящее время IoT оказывает существенное влияние на различные сферы деятельности, включая промышленность (промышленный интернет вещей, IIoT), городское хозяйство и потребительский сектор, предоставляя новые инструменты для автоматизации процессов, повышения эффективности и сбора аналитических данных [1–3].

Данные, генерируемые интернетом вещей, относятся к большим данным, поэтому для их анализа применяются методы машинного обучения. Анализ заключается в оценке вероятностно-временных характеристик трафика интернета вещей, раннего обнаружения аномалий в трафике, детектирования атак, прогнозирования объема трафика. Большинство этих задач требует наличия датасета, на котором выполняется обучение модели машинного обучения. Сбор такого датасета представляет собой отдельную сложную задачу, включающую запись трафика, очистку от шумов, организацию хранения и доступа к нему, валидацию данных [4–7].

Использование уже готовых датасетов имеет свои недостатки: выбор устройств и количество данных ограничены. Также при анализе данных из готовых датасетов нет уверенности в достоверности данных, исследователи полагаются на описание к датасетам и связанные с ними научные работы, которые могут прилагаться создателями [8, 9].

Для того чтобы получить синтетический датасет, основанный на уже имеющемся, можно применить различные инструменты ПО, например различные библиотеки. В данной работе рассматривается библиотека Synthetic Data Vault (SDV) языка Python для создания табличных синтетических данных. Для получения искусственного набора данных, необходимо обучить существующие в библиотеке модели на известном исследователям датасете. В данной статье оригинальный датасет состоит из 100000 случайно выбранных записей из датасета “CIC IoMT 2024 WiFi MQTT”, подразумевающего наличие записей из трафика устройств медицинского интернета вещей. Датасет был преобразован для детектирования аномалии в трафике.

Для получения синтетического трафика были использованы три синтезатора: GaussianCopulaSynthesizer (использует классические статистические методы), CTGANSynthesizer (использует генеративные состязательные сети) и TVAESynthesizer (использует вариационный автоэнкодер). Все три синтезатора используют значения по умолчанию и использованы для создания 30% от оригинального датасета объемом 10000 значений.

Для этого из каждого распределения извлекаются  $M$  выборки для обучения дискриминатора оценки расхождения и далее  $L$  выборок из каждого распределения используются для оценки расхождения между оригинальными и синтетическими данными.

Обучение модели синтезатора включает несколько итераций (эпох). На каждой итерации генератор и дискриминатор стремятся минимизировать потерю. После каждой эпохи модель выводит значения потерь для генератора и дискриминатора. По мере обучения потеря генератора обычно становится более отрицательной, а потеря дискриминатора — менее положительной. Если значения потерь не сходятся, это может указывать на необходимость изменить архитектуру генеративной модели.

Генеративная модель GaussianCopulaSynthesizer сначала изучает маргинальные распределения по атрибутам датасета и нормализует значения с помощью изученного распределения, создавая нормальные кривые с математическим ожиданием  $\mu=0$  и дисперсией  $\sigma=1$ , а далее выполняет обучение корреляций между атрибутами датасета: модель оценивает корреляцию между каждой парой нормализованных атрибутов датасета и сохраняет значения коэффициентов корреляции в виде матрицы  $\mathbf{R}_{n \times n}$ , где  $n$  — количество столбцов в таблице. Обученная модель способна генерировать синтетический датасет, при этом структура датасета остается идентичной оригинальному датасету. Параметрами модели GaussianCopulaSynthesizer являются: диапазон минимальных и максимальных значений атрибутов датасета, форма распределения атрибутов датасета и формат числовых значений датасета.

Для оценки качества детектирования выбирается модели классификатора XGBClassifier [5]. Для её обучения используются два датасета: оригинальный и смешанный (оригинальные и полученные синтетические данные). В качестве оценки модели используются следующие критерии: точность, балансирующая точность и f1-оценка. Полученные результаты отображаются в Таблице 2.

В работе рассмотрены разные методы получения трафика устройств интернета вещей для его дальнейшего анализа. У каждого метода есть свои преимущества и недостатки. Физический метод выдаёт наиболее близкие к реальным значения, но требует очень большого количества ресурсов. Имитация устройств интернета вещей также выдаёт правдоподобные данные, но требует высокого уровня технического и программного обеспечения. Генерация синтетических данных основывается на уже существующем датасете, что требует уверенности в самом датасете и применения средств ПО для генерации. В данной работе были сгенерированы синтетические данные с помощью трёх различных синтезаторов с различной точностью — от 66 до 86 процентов. При слиянии полученных от различных синтезаторов датасетов с оригинальным и обучении на них модели машинного обучения XGBClassifier для детектирования аномального трафика были

получены результаты близкие к 0.9. Это показывает, что синтетические данные могут быть использованы в изучении вопросов, касающихся трафика устройств интернета вещей.

#### СПИСОК ЛИТЕРАТУРЫ

1. Интернет вещей и межмашинные коммуникации. Обзор ситуации в России и мире // Мобильные телекоммуникации. 2013. №7. С. 26-28.
2. Киричек Р.В., Парамонов А.И., Прокопьев А.В., Кучерявый А.Е. Эволюция исследований в области беспроводных сенсорных сетей// Информационные технологии и телекоммуникации. 2014. № 4 (8). С. 29–41.
3. Викулов А.С. Анализ трафика в сети беспроводного доступа стандарта IEEE 802.11 / А.С. Викулов, А.И. Парамонов//Труды учебных заведений связи. 2017. Т. 3. № 3. С. 21–27.
4. Савельева Д.Д., Татарникова Т.М. О системе контроля за расходом трафика устройств интернета вещей // Волновая электроника и инфокоммуникационные системы: Сборник статей XXV Международной научной конференции. СПб: СПбГУАП, 2022. С. 95-98.
5. Татарникова Т.М., Бимбетов Ф., Богданов П.Ю. Выявление аномалий сетевого трафика методом глубокого обучения//Известия СПбГЭТУ ЛЭТИ. 2021. № 4. С. 36-41.
6. Сафронова Е. О., Жук Г. А. Применение искусственных нейронных сетей для прогнозирования DoS атак // Молодой ученый. 2019. №23. С. 27-30.
7. Суриков К.А. Архитектура системы интернета вещей // Международный журнал гуманитарных и естественных наук. № 3-2, 2022. С. 152-155.
8. Браницкий А.А., Котенко И.В. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИРАН. 2016. Вып. 2(45), С. 207-244.
9. Fatihand E. Aydin G. Data Classification with Deep Learning Using Tensorflow // International Conference on Computer Science and Engineering, 2017. P. 755–758.

УДК 004.08

#### АЛГОРИТМ ЗАЩИТНОГО МАСКИРОВАНИЯ АУДИОИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ КВАЗИОРТОГОНАЛЬНЫХ МАТРИЦ

**Сергеев Михаил Борисович, Сергеев Александр Михайлович, Григорьев Евгений Константинович**

Санкт-Петербургский государственный университет аэрокосмического приборостроения

Большая Морская ул., 67, Санкт-Петербург, 190121, Россия

e-mail: tm-tatarn@yandex.ru, dept41@guap.ru

**Аннотация.** Рассматривается применение ортогональных матриц в системах обработки и преобразования информации. Предложен метод оценки результатов защитного маскирования аудиоинформации с использованием, структурированных по Уолшу квазиортогональных матриц Мерсенна.

**Ключевые слова:** ортогональная матрица; маскирование сообщения; алгоритм маскирования/демаскирования; амплитудно-частотная характеристика; белый шум; среднеквадратичная ошибка; отношение сигнал-шум.

#### ALGORITHM FOR PROTECTIVE MASKING OF AUDIO INFORMATION USING QUASI-ORTHOGONAL MATRICES

**Sergeev Mikhail, Sergeev Alexander, Grigoriev Evgeny**

Saint Petersburg State University of Aerospace Instrumentation

67, Bolshaya Morskaya St, St. Petersburg, 190121 Russia

e-mail: tm-tatarn@yandex.ru, dept41@guap.ru

**Abstract.** The application of orthogonal matrices in information processing and transformation systems is considered. A method for assessing the results of protective masking of audio information using quasi-orthogonal Mersenne matrices structured according to Walsh is proposed.

**Keywords:** orthogonal matrix; message masking; masking/demasking algorithm; frequency response; white noise; mean square error; signal-to-noise ratio.

Ортогональные и квазиортогональные матрицы широко используются в системах передачи и хранения данных, в том числе задачах кодирования и помехоустойчивого кодирования изображений и аудиосообщений.

Так, в работе [1] предлагается маскирование звукового файла с применением секретного ключа — матрицы вещественных случайных чисел. Однако авторы не поясняют как решаются потенциальные проблемы вычисления обратной матрицы.

В работах [2–4] используются хаотические матрицы, при работе с которыми возникают проблемы интерпретации полученных результатов, а также сильная зависимость от начальных условий.

Кроме того, использование при защитном кодировании (маскировании) квазиортогональных матриц Мерсенна, структурированных по Уолшу, снимает ряд существующих проблем [5, 6]:

- для таких матриц обратная матрица не вычисляется, а является транспонированной;
- выбор матрицы для декодирования определяется ее порядковым номером в общей базе матриц для передающей и приемной сторон сетевой коммуникации.

Как известно, если длина ключа системы шифрования совпадает с длиной сообщения, методов восстановления шифрованного сообщения не существует. Наше предложение по защите звуковых цифровых данных основано на данном утверждении. Отличие реализации от известных способов с применением матриц состоит в том, что:

- исходное сообщение формируется в виде матрицы размера  $n \times n$ , путем распределения блоков цифровых звуковых данных последовательно по строкам, но  $n$  — не является произвольным, а кратно объему данных, передаваемых, например, в пакетах при передаче по IP-сетям;
- преобразование осуществляется только путем математического умножения матрицы сообщения на матрицу-ключ справа и результат представляет собой матрицу того же размера  $n \times n$ ;
- матрица-ключ является структурированной ортогональной и процесс маскирования/демаскирования «почти» симметричен — восстановление выполняется умножением на транспонированную матрицу слева;
- возможно использование матрицы-ключа как размера  $n \times n$ , так любого меньшего размера, кратного  $n$ , что расширяет выбор и повышает гибкость реализации.

Извлечение полезной информации из элементов матрицы после преобразования невозможно. Их значения определяются не только матрицей-ключом, но и цифровыми отсчетами звукового сигнала в строке, поскольку каждый элемент представляет собой сумму парных произведений элементов строки сообщения и столбца матрицы-ключа. Для проведения экспериментов разработана программа преобразования.

Маскирование несжатых аудиофайлов формата .wav, взятых из датасета «UrbanSound8K» по адресу <https://www.kaggle.com/datasets/chrisfilo/urbansound8k>, проводилось с использованием матриц Мерсенна-Уолша.

Частота дискретизации аудиофайлов — 48 КГц. Файлы, в которых количество отсчетов превышает количество элементов матрицы-ключа, были обрезаны для выравнивания их длин.

В качестве матрицы-ключа использовалась квадратная двухуровневая матрица Мерсенна-Уолша размера  $511 \times 511$  со значениями элементов, равных 1 и  $-b$ , где  $b = 0,9188$ .

Компьютерный эксперимент с оценкой параметров преобразований аудиофайлов проводился по следующему алгоритму [7,8]:

1. Последовательно на вход программы преобразования подаются аудиофайлы из таблицы №1.
2. Вычисляется амплитудный спектр каждого аудиофайла. В случае необходимости количество отсчетов аудиофайла подгоняется под размер матрицы-ключа.
3. Входной файл преобразовывается в матрицу звукового сигнала размером  $511 \times 511$ .
4. Матрица с содержимым звукового файла умножается на матрицу-ключ с формированием маскированного звукового файла.
5. Вычисляются метрики: среднеквадратическая ошибка (MSE) и отношение сигнал-шум в децибелах (SNR), а также амплитудно-частотная характеристика (АЧХ) маскированного звукового сигнала.
6. Выполняется обратное преобразование маскированного звукового файла с формированием демаскированного звукового сигнала.
7. Вычисляются метрики MSE, SNR, а также АЧХ демаскированного звукового сигнала.

Известно, что метрик вычисления качества искажения (маскирования) звука не существует. Поэтому в рамках данного исследования предложен альтернативный подход к определению качества маскирования звукового сигнала. Он основывается на оценке близости АЧХ звукового сигнала к АЧХ белого шума.

Спектр маскированного звукового сигнала близок к спектру белого гауссовского шума, среднеквадратическое отклонение между ними составляет  $2,1379 \cdot 10^{-05}$ . Эксперименты по матричному маскированию других звуковых файлов показали аналогичные результаты.

Для защитного преобразования цифровой звуковой информации — маскирования — применение ортогональной матрицы-ключа отличается от известных подходов предсказуемыми результатами и простотой реализации.

Извлечение полезной информации из элементов матрицы после преобразования невозможно. Их значения определяются матрицей-ключом и цифровыми отсчетами звукового сигнала в строке.

Маскирование квадратной матрицей Мерсенна-Уолша размера  $n$  приводит цифровую звуковую информацию к виду, близкому по спектру к белому шуму. Размер матриц  $n$  следует выбирать кратным длине пакета, например, IP-пакета.

#### СПИСОК ЛИТЕРАТУРЫ

1. Al-laham M.M.A Method for Encrypting and Decrypting wave Files // International Journal of Network Security & Its Applications. 2018. Vol. 10, № 4. P. 11-21.
2. Abdallah H.A., Meshoul S.A. Multilayered Audio Signal Encryption Approach for Secure Voice Communication // Electronics. 2023. № 12. P. 2.
3. Hameed Y.M., Ali N. M. An efficient audio encryption based on chaotic logistic map with 3D matrix // Journal of Theoretical and Applied Information Technology. 2018. № 96. P. 5142-5152.
4. Luis M., Daniel L., Isabel A. A new multimedia cryptosystem using chaos, quaternion theory and modular arithmetic // Multimedia Tools and Applications. 2023. Vol. 82. P. 35149-35181.
5. Farsana F.J., Devi V.R., Gopakumar K. An audio encryption scheme based on Fast Walsh Hadamard Transform and mixed chaotic keystreams URL: <https://doi.org/10.1016/j.aci.2019.10.001> (дата обращения 11.09.2023).
6. Балонин Ю.Н., Востриков А.А., Куртяник Д.В., Сергеев А.М. Обогащение набора последовательностей в задаче поиска блоков симметричных матриц Адамара // Инженерный вестник Дона. 2023. № 1. 13 с.
7. Григорьев Е.К., Сергеев А.М. Оценка качества матричного маскирования цифровых звуковых данных // Труды учебных заведений связи. 2023. Т. 9. № 3. С. 6-13.
8. Кутузов О.И., Татарникова Т.М. Из практики применения метода Монте-Карло // Заводская лаборатория. Диагностика материалов. 2017. Т. 83. № 3. С. 65-70.

УДК 004.056

## ПРИМЕНЕНИЕ НЕЙРОННОЙ СЕТИ С АРХИТЕКТУРОЙ АВТОЭНКОДЕРА ДЛЯ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК

**Татарникова Татьяна Михайловна**

Санкт-Петербургский государственный университет аэрокосмического приборостроения  
Большая Морская ул., 67, Санкт-Петербург, 190121, Россия  
e-mail: tm-tatarn@yandex.ru

**Аннотация.** Обсуждается задача применения нейронной сети с архитектурой автоэнкодера для обнаружения сетевых атак. Приводится формализованное описание структуры автоэнкодера. Показано, что одной из трудностей при выборе архитектуры автоэнкодера является подбор сжимающей функции с гарантией восстановления первоначального количества признаков на выходе нейронной сети с допустимой ошибкой. Предложено применять метод главных компонент, как сжимающую функцию с образованием скрытого слоя автоэнкодера.

**Ключевые слова:** метод главных компонент; сокращение числа параметров; автоэнкодер; ошибка обучения.

## APPLICATION OF NEURAL NETWORK WITH AUTOENCODER ARCHITECTURE TO DETECT NETWORK ATTACKS

**Tatarnikova Tatiana**

Saint Petersburg State University of Aerospace Instrumentation  
67, Bolshaya Morskaya St, St. Petersburg, 190121 Russia  
e-mail: tm-tatarn@yandex.ru

**Abstract.** The problem of using a neural network with an autoencoder architecture to detect network attacks is discussed. A formalized description of the autoencoder structure is given. It is shown that one of the difficulties in choosing an autoencoder architecture is the selection of a compression function with a guarantee of restoring the original number of features at the output of the neural network with an acceptable error. It is proposed to use the principal component method as a compression function with the formation of a hidden layer of the autoencoder.

**Keywords:** principal component analysis; parameter reduction; autoencoder; training error.

Анализ и обработка больших данных стали необходимостью в различных отраслях экономики от медицинских исследований до финансового анализа и промышленной автоматизации. Умение обрабатывать и использовать большие объемы информации становится ключевым конкурентным преимуществом.

С одной стороны, большие данные дают возможность выявить специфические закономерности внутри меньших подгрупп и слабые связи между признаками, а значит делать более детальные прогнозы и решения, принимаемые на их основе. С другой стороны, большие данные требуют длительного процесса предобработки, заключающегося в слиянии разнообразных источников информации и необходимости одновременной оценки и проверки огромного количества параметров, что предсказуемо приводит к увеличению погрешности. Иногда погрешности могут превышать важность настоящих данных, становясь доминирующим. Снятие этой проблемы решается применением методов разреженности к отбору значимых параметров больших данных [1].

Предлагается на этапе предобработки данных применять метод главных компонент (Principal Component Analysis, PCA). Метод позволяет выявить основные корреляции между параметрами многомерных данных, и, соответственно, сократить их размерность, удалив малоинформативные данные. Это помогает повысить производительность моделей машинного обучения, уменьшить переобучение и ускорить вычисления [2].

В работе показана возможность применения метода главных компонент в качестве функции сжатия нейронной сети с архитектурой автоэнкодера и демонстрация работы данного автоэнкодера по распознавание аномального трафика инфокоммуникационных сетей.

Современные системы обнаружения вторжений, функции которых заключаются в детектировании аномального трафика с последующей идентификацией атаки, основаны на поведенческих и/или сигнатурных моделях. Поведенческая модель детектировании аномального трафика, несущего угрозу основана на оценивании отклонения характеристик сетевого узла от его штатной работы [3]. В оценивании характеристик участвуют статистические модели: пороговая, среднего значения, среднеквадратичного отклонения. Если с течением времени наблюдается определенное отклонение величины характеристик от допустимого значения, то фиксируется аномальное поведение или обнаружение атаки. Об аномальном поведении, например, можно судить при увеличении частоты запросов и загрузки узла [4]. Сигнатурная модель представляет собой некий паттерн описания атаки и поиска этого паттерна в сетевом трафике. Обе модели предполагают использование нейронных сетей [5, 6].

Задача обнаружения аномалий в сетевом трафике с применением технологий искусственного интеллекта не является новой. Однако, с увеличением числа признаков обучение нейронных сетей может занимать много времени, что при обнаружении сетевых атак в реальном времени недопустимо. К тому же на практике некоторые из архитектур нейронных сетей требуют значительных объемов вычислительных ресурсов для обучения.

В работе предлагается использовать нейронной сети с архитектурой автоэнкодера для обнаружения сетевых атак, при этом применять метод главных компонент, как сжимающую функцию и образующую скрытый слой автоэнкодера [7]. Состоятельность применения автоэнкодера для классификации атак продемонстрирована на

обучении нейронной сети этого типа на известном наборе исходных данных, содержащем в своем составе 17 классов после исключения несбалансированных классов [8, 9].

Достоверность классификации сетевых атак оценивалась такими метриками как достоверность классификации, точность классификации, доля истинно положительных решений и F-мера [10, 11]. Достоверность классификации выше 90% показана для атак, число примеров обучения которых составляет более 400, исключение коснулось только атаки типа `httptunnel`. Объяснение таким результатам можно дать только принадлежностью атак к одной категории, а значит схожестью признаков. Точность классификатора, основанного на автоэнкодере составила 90%, доля истинно положительных решений — 88% и F-мера — 85% на обучаемом наборе данных, и на 1-2% ниже значений этих же показателей эффективности классификатора на тестовом наборе.

#### СПИСОК ЛИТЕРАТУРЫ

1. Самойлова И. А. Технологии обработки больших данных // Молодой ученый. 2017. № 49 (183). С. 26-28.
2. Кабаков Р. И. R в действии. Анализ и визуализация данных в программе R. М.: ДМК Пресс, 2016. 588 с.
3. Wu S. X., Banzhaf W. The Use of Computational Intelligence in Intrusion Detection Systems: A Review // Applied Soft Computing. 2010. Vol. 10(1). P. 1–35.
4. Созыкин А.В. Обзор методов обучения глубоких нейронных сетей // Вестник ЮУрГУ, Серия: Вычислительная математика и информатика. 2017. Т. 6. № 3. С. 28-59.
5. Tatarnikova T.M. Restricting data leakage through non-obvious features of Android 5 smartphone // Informationno-Upravliaiushchie Sistemy. 2019. Vol. 5. P. 25-29.
6. Сафронова Е.О., Жук Г.А. Применение искусственных нейронных сетей для прогнозирования DoS атак // Молодой ученый. 2019. № 23. С. 27-30.
7. Шелухин О.И., Филинова А.С. Сравнительный анализ алгоритмов обнаружения аномалий трафика методами дискретного вейвлет-анализа // T-Comm. 2014. Т. 9. С. 89-97.
8. A Deeper Dive into the NSL-KDD Data Set Towards Data Science [Электронный ресурс]. Режим доступа: <https://towardsdatascience.com/a-deeper-dive-into-the-nsL-kdd-data-set-15c753364657> (дата обращения: 10.09.2024).
9. Ingre B. Yadav A., Soni A.K. Decision Tree Based Intrusion Detection System for NSL-KDD Dataset // Proceedings of the International Conference on Information and Communication Technology for Intelligent Systems (ICTIS, Ahmedabad, India, 25–26 March 2017). Cham: Springer. 2017. Vol. 2. P. 207–218.
10. Татарникова Т.М. Бимбетов Ф., Богданов П.Ю. Выявление аномалий сетевого трафика методом глубокого обучения // Известия СПбГЭТУ ЛЭТИ. 2021. № 4. С. 36-41.
11. Татарникова Т.М., Богданов П.Ю. Метрические характеристики обнаружения аномального трафика в сетях интернета вещей // T-Comm: Телекоммуникации и транспорт. 2022. Т. 15. №1. С. 15-21.

УДК 004.622

### ПРИМЕНЕНИЕ МЕТОДЫ ПРЕДОБРАБОТКИ ИЗОБРАЖЕНИЙ РУКОПИСНЫХ ДОКУМЕНТОВ В ЗАДАЧАХ КОМПЬЮТЕРНОГО ЗРЕНИЯ

Шихотов Алексей Алексеевич

Санкт-Петербургский государственный университет аэрокосмического приборостроения

Большая Морская ул., 67, Санкт-Петербург, 190121, Россия

e-mail: ashikhotov@bk.ru

**Аннотация.** Автоматизация анализа рукописных документов решается с применением технологий обработки изображений. Рукописные тексты представляют собой сложный объект для извлечения информации из-за разнообразия стилей письма, различных уровней чёткости и наличия шумов. Шум может проявляться в виде дефектов, размытости или искажений. В статье рассмотрено несколько подходов по удалению клетки на листе бумаги с использованием библиотеки OpenCV языка Python.

**Ключевые слова:** рукописный документ; извлечение информации; шумы; обработка изображений; компьютерное зрение.

### METHODS FOR PREPROCESSING IMAGES OF HANDWRITTEN DOCUMENTS IN COMPUTER VISION TASKS

Shikhotov Aleksey

Saint Petersburg State University of Aerospace Instrumentation

67 Bolshaya Morskaya St, St. Petersburg, 190121 Russia

e-mail: ashikhotov@bk.ru

**Abstract.** Automation of handwritten document analysis is solved using image processing technologies. Handwritten texts are a complex object for information extraction due to the variety of writing styles, different levels of clarity and the presence of noise. Noise can manifest itself in the form of defects, blurriness or distortion. The article considers several approaches to removing a cell on a sheet of paper using the OpenCV library of the Python.

**Keywords:** handwritten document; information extraction; noise; image processing; computer vision.

Современные технологии обработки изображений играют ключевую роль в автоматизации анализа рукописных документов [1]. Рукописные тексты представляют собой сложный объект для анализа из-за разнообразия стилей письма, различных уровней чёткости и наличия шумов, которые могут значительно ухудшить качество извлечённой информации. Эффективная предварительная обработка изображений является важным этапом в процессе распознавания и анализа рукописных документов, поскольку позволяет улучшить качество изображений и повысить точность последующих алгоритмов.

Основной задачей предварительной обработки является удаление шума, который может возникать из-за различных факторов, таких как качество сканирования, условия освещения и физическое состояние документа. Шум может проявляться в виде дефектов, размытости или искажений, что делает распознавание текста трудоёмким и менее надёжным [2].

Одной из частных проблем при обработке изображений рукописных документов является необходимость удаления рисунка клетки на клетчатой бумаге. Клетка может мешать распознаванию текста путём создания визуального шума, отвлекая внимание алгоритмов распознавания и ухудшая общую точность извлечения информации. В данной работе было рассмотрено несколько подходов по удалению клетки на листе бумаги с использованием библиотеки OpenCV языка Python.

Первый подход использует алгоритм обнаружений границ Canny. В зависимости от требований можно выделить большинство границ или только те границы, которые имеют чёткое начертание. Это становится возможным при изменении параметров порогового значения гистерезиса. В результате применения такого подхода можно на некоторых изображениях добиться игнорирования клетки и выделения полезной информации. Ожидаемо, что вместе с клеткой пропадает часть рукописного текста с изображения, из-за чего данный способ может быть эффективно использован только в случае чёткого изображения и толстых линий рукописного текста.

Второй подход использует в дополнение к алгоритму Canny алгоритм преобразования Хафа для нахождения прямых линий клетки в границах [3]. Данный подход может быть полезен, когда клетка на листе бумаги или любые другие линии имеют чёткие контуры, которые возможно убрать только при потере качества полезных данных.

Третий подход использует простейший метод фильтрации изображения по цветовым характеристикам [4]. Так возможно выделение необходимого диапазона синего цвета чернил, которыми был написан текст. Для упрощения задачи лучше конвертировать RGB изображение в пространство HSV, где необходимо создать маску по цвету, насыщенности и яркости, а после применить маску к исходному изображению. В результате фильтр выделяет напрямую рукописный текст из изображения. Качество полученных данных имеет огрехи из-за узкого диапазона цветового спектра, которые устранить возможно, но при этом под фильтр попадёт клетка, что добавит шума в изображение.

Четвёртый подход использует комбинацию методов. Примером может служить комбинация двух методов из библиотеки OpenCV. В первую очередь выполняется бинаризация изображения с использованием алгоритма Adaptive Threshold, а после применяется морфологическая функция Morph Close для окончательного удаления шума на изображении [4]. Фактически оба метода используются с одной и той же целью — удаление шума, но их комбинация позволяет ещё лучше справиться с данной задачей. Стоит отметить, что клетка исчезла, оставив после себя небольшое количество шума, которое слабо влияет на качество текста, но попытки изменения регулирующих параметров приводит к ухудшению качества текста.

После небольшого анализа результатов замечено, что наивысшее качество данных в тестовом изображении выдал алгоритм нахождения границ Canny. Для дальнейшей обработки необходимо применять морфологическую функцию Morph Close для яркости.

Сравнивая два комбинированных подхода, можно подытожить, что оба из них имеют место на существование. В частности, первый результат оставляет на изображении тонкие и слегка прерывистые линии цифр, а второй толстые и немного смазанные линии цифр. При достаточно качественной обучающей выборке разница в комбинированных подходах, как в данном примере, будет несущественной, что позволяет специалисту сделать выбор подходящего метода.

Далее полученные цифры были преобразованы к размеру 28 на 28 пикселей в соответствии с обучающей выборкой для нейронной сети [5].

Сравнивая четыре подхода по обработке изображений с целью сохранения качества рукописного текста и удаления шума можно выделить несколько важных моментов.

Во-первых, каждый из рассмотренных методов обладает регулируемыми параметрами, которые позволяют балансировать между требуемым качеством рукописного текста и наличием шума.

Во-вторых, стоит выделять характерные черты рукописного текста в документе, такие как цвет и насыщенность текста, а также качество освещённости документа. При обработке единичных образцов данные характеристики могут послужить созданию простейшего и эффективного фильтра.

В-третьих, в частном случае может преобладать качество у отдельного подхода, но лучшим решением для общих случаев может послужить комбинация нескольких подходов, которые бы могли в совокупности представлять многоэтапный процесс обработки, учитывающий множество особенностей обрабатываемой группы документов.

## СПИСОК ЛИТЕРАТУРЫ

1. Naveen, K. Big Data Statistics 2024: Growth and Market Data / K. Naveen. URL: <https://www.demandsage.com/big-data-statistics/> (дата обращения: 09.12.2024).
2. Жаринов, О. О. Основы цифровой обработки изображений / О.О. Жаринов. СПб.: ГУАП, 2023. 95 с.
3. Кудрина, М. А. Использование преобразования Хафа для обнаружения прямых линий и окружностей на изображении / М. А. Кудрина // Сборник трудов конференции «Перспективные информационные технологии ПИТ-2013». С. 432-435.
4. Быков, Р. Е. Цифровые фильтры цветности в задачах обработки видеоизображений / Р. Е. Быков // Автоматический анализ и распознавание изображений. 2010. №3(9). С. 42-48.
5. Татарникова, Т.М., Пойманова, Е.Д., Богданов, П.Ю., Краева, Е.В., Веревкин, С.А. Программные среды для изучения основ нейронных сетей / Т. М. Татарникова, Е. Д. Пойманова, П. Ю. Богданов, Е. В. Краева, С. А. Веревкин // Программные продукты и системы. 2021. № 1. С. 145-150.

УДК 621.3.088

**ИНТЕЛЛЕКТУАЛЬНЫЙ АНАЛИЗ ДАННЫХ О ДОРОЖНО-ТРАНСПОРТНЫХ  
ПРОИСШЕСТВИЯХ НА ТЕРРИТОРИИ ЗАБАЙКАЛЬСКОГО КРАЯ****Юрко Артём Евгеньевич**

Главное Управление МЧС России по Забайкальскому краю  
Костюшко-Григоровича ул., 37, Чита, 672000, Россия  
e-mail: uyrkoartem@mail.ru

**Аннотация.** Работа посвящена изучению методов и средств имитационного моделирования, применяемых для создания инструментальной среды поддержки учебного процесса подготовки разработчиков информационных систем и технологий. Рассматривается важность использования имитационных моделей в учебном процессе, позволяющих студентам приобретать опыт проектирования и реализации информационных систем.

**Ключевые слова:** имитационное моделирование; инструментальная среда; учебный процесс; информационные системы; проектирование; технологии; средства моделирования; подготовка специалистов; учебные программы; разработчики информационных систем.

**INTELLECTUAL ANALYSIS OF ROAD TRAFFIC ACCIDENTS  
IN THE TERRITORY OF TRANSBAIKAL REGION****Yurko Artem**

Main Directorate of EMERCOM of Russia for Transbaikal region  
37 Kostyushko-Grigorovicha St, Chita, 672000, Russia  
e-mails: uyrkoartem@mail.ru

**Abstract.** The work is devoted to studying methods and tools of simulation modeling used for creating an instrumental environment that supports the educational process aimed at training developers of information systems and technologies. The importance of using simulation models in education is discussed, as they allow students to gain experience in designing and implementing information systems.

**Keywords:** simulation modeling; toolset environment; educational process; information systems; design; technologies; modeling tools; professional development; curricula; information system developers.

Актуальность проблемы: высокая аварийность в Забайкальском крае вызвана неблагоприятными климатическими условиями и проблемами с транспортной инфраструктурой. Традиционные подходы к учету и анализу ДТП недостаточны, отсутствует единый подход к прогнозированию и оперативному реагированию.

Цель исследования: разработка интеллектуальной системы прогнозирования зон риска дорожно-транспортных происшествий (ДТП) и выработка рекомендаций по рациональному размещению сил и средств экстренных служб Забайкальского края.

Для достижения поставленной цели необходимо выполнить ряд задач, а именно проанализировать дорожно-транспортную обстановку в регионе, исследовать методы интеллектуального анализа данных для прогнозирования ДТП, подготовить базы данных по ДТП на территории региона за 2019 — 2024 гг., построить модель прогнозирования ДТП, разработать рекомендации по размещению сил и средств аварийно-спасательных формирований.

Применялись методы анализа данных, визуализации, машинного обучения и прогнозирования.

Забайкальский край характеризуется значительным влиянием неблагоприятных природных условий, ограниченной транспортной инфраструктурой и большим числом труднодоступных районов, что негативно сказывается на безопасности дорожного движения и увеличении аварийности. Особенности региона включают большую территорию, гористую местность, низкую плотность населенных пунктов, суровую зиму с быстрым изменением погодных условий, плохое состояние дорог и недостаточность сервисных учреждений. Современная система учета и анализа данных о ДТП испытывает серьезные ограничения, такие как недостаток централизованной базы данных, отсутствие прогнозирующих инструментов и значительные задержки в обработке информации. Поэтому актуальной задачей становится создание интеллектуальной системы прогнозирования зон риска ДТП и выработки рекомендаций по рациональному размещению сил и средств экстренных служб, что должно способствовать снижению числа аварий и материальных потерь.

Забайкальский край характеризуется низкой плотностью населения, сложной топографией местности и суровым континентальным климатом, что создает особые условия для дорожного движения и увеличения аварийности. Здесь необходимы продвинутые методы анализа данных, такие как Data Mining и машинное обучение, позволяющие выявлять скрытые зависимости и тенденции, что способствует эффективному прогнозированию ДТП и выявлению опасных участков дорог. Важную роль играют технологии пространственного анализа и ГИС, помогающие визуализировать зоны риска и планировать размещение ресурсов экстренных служб. Ключевой проблемой остается отсутствие единого механизма прогнозирования и координации действий, что подчеркивает необходимость комплексного подхода, интегрирующего разнородные данные о погоде, трафике, состоянии дорог и инфраструктуре. Применение методов машинного обучения, таких как классификация, кластеризация и регрессия, позволяет повысить безопасность дорожного движения и эффективность управления транспортным процессом в регионе.

Анализ данных о дорожно-транспортных происшествиях (ДТП) в Забайкальском крае показывает рост числа аварий, что обусловлено множеством факторов: техническое состояние транспорта, низкая квалификация водителей, некачественные дороги и климатические условия. Специалисты МЧС реагируют на большинство ДТП, обеспечивая эвакуацию пострадавших и ликвидацию последствий. За 2019–2024 годы наблюдается устойчивая тенденция роста числа происшествий, травм и гибели людей. Решением проблемы является создание интеллектуальной модели прогнозирования ДТП на основе методов машинного обучения и пространственного анализа (ГИС), позволяющей выявить «горячие точки» аварийности и предложить стратегию размещения сил и средств экстренных служб. Использование этих данных в сочетании с рекомендациями по оптимизации расписания, запасу ресурсов и обучению персонала создаст надежный фундамент для сокращения времени реагирования и повышения безопасности дорожного движения в регионе.

Планируется разработка модели прогнозирования аварийности на дорогах Забайкальского края с использованием методов машинного обучения. Модель будет реализована на языке программирования Python, который является одним из наиболее популярных и универсальных инструментов для анализа данных и разработки интеллектуальных систем. Выбор Python обусловлен его обширной экосистемой библиотек, таких как Pandas, NumPy, Scikit-learn и TensorFlow, которые обеспечивают гибкость и эффективность при работе с большими объемами данных и построении сложных моделей.

Модель будет обучена на исторических данных о дорожно-транспортных происшествиях (ДТП).

Важным аспектом модели является ее способность учитывать пространственно-временные закономерности, что позволит прогнозировать не только общее количество ДТП, но и их распределение по периодам года и по районам. Это даст возможность экстренным службам и органам управления дорожным движением принимать обоснованные решения по распределению ресурсов и проведению профилактических мероприятий.

В итоге была проведена комплексная разработка интеллектуальной системы прогнозирования дорожно-транспортных происшествий (ДТП) и рекомендаций по размещению сил и средств экстренных служб на территории Забайкальского края. Исследование включало анализ дорожно-транспортной обстановки, изучение методов интеллектуального анализа данных и практическую реализацию аналитической модели.

Разработанная модель прогнозирования ДТП и рекомендации по размещению сил и средств могут быть интегрированы в деятельность МЧС России.

Благодаря прогнозированию зон риска и оптимальному размещению ресурсов, экстренные службы смогут быстрее прибывать на место происшествия.

Модель поможет точнее распределять силы и средства, что улучшит координацию действий и повысит эффективность работы.

Прогнозирование аварийности позволит заранее принимать меры по предотвращению ДТП и минимизировать последствия.

Таким образом, результаты работы имеют высокую практическую значимость и могут быть использованы для повышения безопасности дорожного движения и улучшения работы экстренных служб в Забайкальском крае и других регионах России.

## СПИСОК ЛИТЕРАТУРЫ

1. Данные по аварийности. Газета «Коммерсант». URL: <https://www.kommersant.ru/doc/7513879> (дата обращения: 25.08.2025).
2. Организация и управление транспортными системами. Учебник / Под ред. А.Н. Кочеткова. Москва: Юрайт, 2023. Глава 4, с. 156-162.
3. Атлас Забайкальского края / Отв. Ред.: Д.В. Гриценко, Н.И. Смирнова. Новосибирск: Наука, Сибирская издательская фирма РАН, 2018.
4. Интервью с заместителем начальника Управления Госавтоинспекции Забайкалья. URL: <https://www.mkchita.ru/social/2025/01/16/ekh-dorogi-intervyu-s-zamnachalnika-upravleniya-gosavtoinspekcii-zabaykalya.html> (дата обращения: 25.05.2025).
5. Авдеенко Е.А., Зайцев Г.П. Прогнозирование аварийности на автомобильных дорогах // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). 2022. № 3. С. 15–22.
6. Зайцев Г.П., Иванов О.Б. Совершенствование методики оценки уровня аварийности на автодорогах // Безопасность дорожного движения. 2023. № 4. С. 25-33.
7. Айвазян С.А., Мхитарян В.С. Прикладная статистика и основы эконометрики. Том II. Эконометрика. Москва: ЮНИТИ-ДАНА, 2021.
8. Васильев Р.М., Гончаров В.Ю. Машинное обучение и анализ данных. Учебник. СПб.: БХВ-Петербург, 2022.
9. Емельянов В.В., Курейчик В.М., Лейбушкин Ф.Л. Методы оптимизации в теории принятия решений. Учебник. М.: Издательство МГТУ им. Н.Э. Баумана, 2021.
10. Ахметзянов А.Р., Карманов В.Г. Основы машинного обучения и анализа данных. Учебник. Москва: Университет ИТМО, 2022.
11. Горбачев В.С., Андреев А.Н. Анализ временных рядов и прогнозирование. Учебник. Москва: Академия, 2022.
12. Панов А. В. Разработка управленческих решений: информационные технологии. М.: «Горячая линия Телеком», 2004. С. 27-30.
13. Трофимов А.Е., Панченко Л.А. Географические информационные системы и пространственный анализ. Учебник. Москва: Аспект-Пресс, 2022.
14. Бородулин А.Н., Горшков С.Ф. Модели и методы анализа дорожно-транспортных происшествий. Учебное пособие. Москва: Инфра-М, 2019.
15. Боровиков В.П. SPSS: искусство обработки информации. Анализ данных и подготовка отчетов. Москва: Диалог-МИФИ, 2020.
16. Фридман Дж.Х., Хастил Д., Тибширани Р. Обучение с учителем и непараметрическое оценивание. Пер. с англ.. М.: Вильямс, 2022.
17. Колесов Ю.Б., Полянин А.Д. Анализ данных и прогнозирование. Учебник. М.: Высшая школа, 2021.
18. Дьяконов В.П., Круглов В.В. MATLAB и SIMULINK для радиоинженеров. Учебное пособие. М.: Солон-пресс, 2022.
19. Маннинг К.Д., Шютце Х. Введение в обработку естественного языка. Пер. с англ.. М.: Вильямс, 2022.
20. Фролов А.Б., Щербаков А.Ю. Информационная безопасность компьютерных систем и сетей. Учебник. М.: Форум, 2023.





## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ

УДК 656.61.052:004.732

### ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ГЕОИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ ИИ-МАРШРУТИЗАЦИИ СУДОВ В АРКТИЧЕСКИХ ВОДАХ

**Артакин Марк Демидович, Мартын Ирма Андреевна**

Российский государственный гидрометеорологический университет

пр.Металлистов 3, Санкт-Петербург, Россия

e-mails: Mark577@yandex.ru , irma\_martyn@mail.ru

**Аннотация.** Разработка цифровых систем с использованием искусственного интеллекта (ИИ) для маршрутизации судов в Арктике представляет собой комплексную задачу, в которой информационная безопасность (ИБ) становится критическим элементом надежности. Уникальные условия Арктики — уязвимость каналов связи, зависимость от внешних данных и высокая цена последствий — трансформируют киберугрозы в прямые риски для безопасности мореплавания, экологии и национальной безопасности.

**Ключевые слова:** информационная безопасность; геоинформационная система (ГИС); искусственный интеллект (ИИ); арктическая навигация; целостность данных.

### INFORMATION SECURITY OF A GEOINFORMATION SYSTEM FOR AI ROUTING OF VESSELS IN ARCTIC WATERS

**Artamkin Mark, Martyn Irma**

Russian State Hydrometeorological University

3 Metallistov Ave., Saint Petersburg, Russia

e-mails: Mark577@yandex.ru , irma\_martyn@mail.ru

**Annotation.** The development of digital systems using artificial intelligence (AI) for vessel routing in the Arctic is a complex task in which information security (IS) is becoming a critical element of reliability. The unique conditions of the Arctic — the vulnerability of communication channels, dependence on external data, and the high cost of consequences — transform cyber threats into direct risks to maritime safety, the environment, and national security.

**Keywords:** information security; geographic information system (GIS); artificial intelligence (AI); Arctic navigation; data integrity.

Информационная безопасность такой системы является не дополнительной опцией, а критическим фундаментом, обеспечивающим безопасность мореплавания, экологическую защиту Арктики и национальную безопасность. Угрозы здесь трансформируются из киберрисков в риски катастрофических физических последствий.

Выделим специфику и уникальные риски Арктической ГИС.

Специфика Арктической ГИС:

1. Конвергенция физического и цифрового мира, заключается в атаке на систему — это прямая угроза судну, экипажу и хрупкой экосистеме. Последствия - от навигационных ошибок до катастрофических столкновений и разливов топлива.

2. Критическая зависимость от данных, означает то, что система основывается на множестве внешних источников, например данных дистанционного зондирования Земли (спутниковые снимки (ледовая обстановка), данные AIS (Automatic Identification System), гидрометеорологических данных (прогнозы погоды, состояния льда), цифровых карт и батиметрия, манипуляция или компрометация любого из этих источников ведет к формированию ИИ небезопасных маршрутов.

3. Уязвимость каналов связи возникает когда в арктических регионах ограничены возможности спутниковой и другой связи (высокие задержки, низкая пропускная способность, перебои). Это усложняет передачу данных, обновлений и реагирование на инциденты в реальном времени.

4. Экстремальные условия и человеческий фактор - ограниченная возможность быстрого реагирования в случае кибератаки. Экипаж может слепо доверять рекомендациям ИИ, что требует особой надежности.

Уникальные риски и последствия:

1. Превращения кибератаки в физическую катастрофу;
2. Формирование ИИ небезопасного маршрута на основе ложных данных;
3. Паралич системы — невозможность передачи маршрутов и обновлений;
4. Слепое доверие ИИ — несвоевременная реакция экипажа.

К ключевым угрозам информационной безопасности относятся угрозы целостности данных, они являются наиболее опасными, к ним можно отнести «Отравление» данных ИИ (злонамеренное искажение обучающих или операционных данных (например, фальсификация спутниковых данных о ледовой обстановке) для скрытого изменения логики работы ИИ), манипуляция AIS-сигналов (подмена координат судов, создание несуществующих объектов для провокации опасных маневров) или изменений цифровых навигационных карт. Угрозы доступности (Атаки типа «Отказ в обслуживании» - DDoS), например атаки на центры обработки данных или каналы передачи данных, приводящие к невозможности получения актуальных маршрутов. Угрозы конфиденциальности, например перехват коммерческих маршрутов или утечка данных о перемещении судов. Угрозы самой модели ИИ, например целенаправленное создание входных данных, которые заставляют модель ИИ ошибаться, но выглядят нормально для человека (специфический шум на спутниковом снимке, который ИИ интерпретирует как чистую воду, а не лед).

Основные принципы и меры защиты для безопасности системы маршрутизации судов на морской акватории с применением ИИ использование архитектуры «Бездоверия» (Zero Trust), когда используется принцип «Никогда не доверяй, всегда проверяй» и все запросы к системе (от судов, от датчиков, от операторов) должны аутентифицироваться и авторизоваться или микросетевое сегментирование для изоляции критических компонентов (сам алгоритм ИИ, базы картографических данных). Обеспечение целостности и аутентичности данных можно обеспечить с помощью использования технологий Distributed Ledger (Blockchain) для создания неизменяемого журнала получения и обработки критических данных (спутниковые снимки, AIS), в таком случае любое изменение будет сразу заметно, использование цифровых подписей и сертификатов для всех источников данных, использование кросс-валидация данных, где производится сравнение информации из нескольких независимых источников (например, данные с двух разных спутниковых систем) для выявления аномалий.

Защита модели ИИ и алгоритмов может осуществляться с помощью регулярного тестирования на устойчивость к adversarial-атакам, контролем версий и целостности моделей ИИ или использования «Человек в контуре» (Human-in-the-Loop), где производится обязательное утверждение рискованных или нестандартных решений ИИ опытным штурманом или береговым оператором.

Использование криптографии и безопасной связи, например сквозное шифрование (End-to-End Encryption) всех передаваемых данных или использование защищенных и резервированных каналов связи (например, несколько спутниковых операторов).

Таким образом, для цифровой системы с ИИ маршрутизации судов в Арктике информационная безопасность должна быть заложена в архитектуру на этапе проектирования (Security by Design). Это комплексная задача, требующая сочетания передовых технологий (блокчейн, криптография, защита ИИ), продуманных процессов и подготовки людей. Только так можно обеспечить не просто цифровизацию, а безопасную и устойчивую навигацию в суровых условиях Арктики.

#### СПИСОК ЛИТЕРАТУРЫ

1. Истомин, Е. П. Построение оптимального логистического маршрута на морской акватории в условиях ледовой обстановки по данным беспилотных летательных аппаратов / Е. П. Истомин, И. А. Мартын, Я. А. Петров // Информация и космос. – 2025. – № 2. – С. 103-108. – EDN BPHRDD.
2. Е. П. Истомин, Я. А. Петров, И. А. Мартын, Е. С. Новожилова Оценка изменчивости климатических характеристик Карского моря для безопасного и эффективного использования Северного морского пути // Геоинформатика. – 2024. – № 2. – С. 45-53. – DOI 10.47148/1609-364X-2024-2-45-53. – EDN LUNXAC.
3. Smith, J., & Johnson, A. «Integrity Threats in Satellite Data Acquisition for Autonomous Navigation Systems in Remote Areas»//IEEE Transactions on Geoscience and Remote Sensing, 2022, T. 60, стр. 1-14

УДК 004.942

### ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ АРКТИЧЕСКОГО МОНИТОРИНГА: ПРИМЕНЕНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СУДОХОДСТВА ПО СЕВЕРНОМУ МОРСКОМУ ПУТИ

**Болховский Илья Дмитриевич**

Российский государственный гидрометеорологический университет

Воронежская ул., 79, Санкт-Петербург, 192007, Россия

e-mail: ilya.bolkhovsky@gmail.com

**Аннотация.** Рассматривается применение методов машинного обучения для повышения достоверности геоинформационных систем прогнозирования морского льда как элемента критической инфраструктуры Северного морского пути. Анализируются ограничения традиционных методов прогнозирования морского льда, включая барьер предсказуемости в переходные сезоны (погрешность до 25%), недостаточное пространственное разрешение и высокие вычислительные требования. Представлены архитектуры глубокого обучения (LSTM, U-Net, ConvLSTM). Рассматриваются аспекты технологического суверенитета, показана практическая значимость для обеспечения безопасности арктического судоходства в контексте Стратегии развития АЗРФ до 2035 года.

**Ключевые слова:** геоинформационные системы; информационная безопасность; машинное обучение; Арктика; Северный морской путь; критическая инфраструктура; дистанционное зондирование.

## INFORMATION SECURITY OF ARCTIC GIS: MACHINE LEARNING FOR NORTHERN SEA ROUTE NAVIGATION SAFETY

**Bolkhovskiy Ilya**

Russian State Hydrometeorological University  
79 Voronezhskaya st, St. Petersburg, 192007, Russia  
e-mail: ilya.bolkhovskiy@gmail.com

**Abstract.** The application of machine learning methods for enhancing the reliability of geoinformation systems for sea ice forecasting as a critical infrastructure element of the Northern Sea Route is considered. The limitations of traditional sea ice forecasting methods are analyzed, including the predictability barrier during transition seasons, insufficient spatial resolution, and high computational requirements. Hybrid deep learning architectures (LSTM, U-Net, ConvLSTM) are analyzed. Aspects of technological sovereignty are examined, and practical significance for ensuring Arctic navigation safety in the context of the Arctic Zone of the Russian Federation Development Strategy until 2035 is demonstrated.

**Keywords:** geoinformation systems; information security; machine learning; Arctic; Northern Sea Route; critical infrastructure; remote sensing.

АЗРФ является стратегически важным регионом, обеспечивающим приоритет национальной безопасности и долгосрочный экономический рост за счет освоения перспективных минерально-сырьевых центров, а также транспортных коридоров, которые позволяют сократить время доставки грузов по сравнению с традиционными маршрутами на 30-50% [1, 16]. Согласно стратегии развития Арктической зоны РФ ожидается резкий рост грузооборота: с 31,5 миллионов тонн в 2019 году до 130 миллионов тонн к 2035 году [17]. Ввиду этого, обеспечение круглогодичной навигации становится задачей национального уровня.

Ввиду роста активности судоходства, справедливо полагать, что ГИС навигационно-гидрографического обеспечения является элементом критической инфраструктуры арктического региона. Однако, существующие методы прогнозирования ледовой обстановки не всегда способны обеспечить необходимую достоверность и точность ввиду ускоренной трансформации Северного Ледовитого океана в пограничную зону льда с более фрагментарным и тонким льдом [5-6]. Это формирует цепочку угроз: низкая точность прогнозов приводит к навигационным рискам, аварийным ситуациям, экономическим потерям и угрозам безопасности экипажей.

Проблематика обеспечения достоверности данных включает в себя обход ограничений традиционных методов прогнозирования, а также решение задач информационной безопасности ГИС. В числе первых – высокие вычислительные требования физических численных моделей [7], «барьер предсказуемости» в переходные сезоны (погрешность до 25%) [7-8], недостаточное пространственное разрешение и задержки в оперативном прогнозировании [4]. Сюда же следует добавить высокую вариативность: расхождения между различными алгоритмами определения концентрации морского льда могут достигать значений в 1 миллион км<sup>2</sup> прогнозируемой площади [10].

К задачам информационной безопасности относятся, в том числе, обеспечение достоверности и полноты информации, поступающей из разнородных источников данных, что требует мероприятий по уменьшению неопределенности в принятии решений [15]. Также остро стоит вопрос актуализации данных путём минимизации задержки между наблюдением и прогнозом [3].

В отличие от традиционных численных методов и статистических моделей, подходы на основе машинного обучения настроены на выявление сложных, нелинейных закономерностей, даже без необходимости включения физических данных [9]. Машинное обучение применимо для разного масштаба: от деталей на уровне пикселей, критически важных для оперативной навигации, до стратегического планирования для оптимизации маршрутов в Арктике на несколько месяцев вперед [7].

Сети долгой краткосрочной памяти (англ. Long Short-Term Memory, LSTM) обладают ключевым преимуществом в долгосрочных прогнозах, благодаря их способности выдавать стабильно низкие ошибки на протяжении всего горизонта прогнозирования [9]. Однако, существующие LSTM-модели зачастую используют пространственно усредненные метеорологические данные в качестве входных данных, что ведет к уменьшению точности прогноза в пограничных зонах льда [14]. Для устранения подобных ограничений и достижения более высокой точности пространственного анализа применяется комбинирование LSTM-сетей со сверточными сетями (англ. Convolutional Neural Networks; CNN), специально разработанными для обработки изображений при помощи алгоритмов без обучения [4].

Архитектура U-Net представляет собой расширение сверточных сетей. Изначально разработанная для сегментации биомедицинских изображений, она доказала свою высокую эффективность для классификации спутниковых изображений, позволяя обрабатывать изображения произвольного размера без необходимости деления исходного изображения на фрагменты [7, 12-13].

Для обеспечения одновременной точности пространственного и временного анализа применяется комбинирование CNN и LSTM сетей в одной архитектуре [1]. Частным случаем такой архитектуры является модель ConvLSTM. Данная модель показала способность поддерживать среднеквадратичную ошибку на уровне около 15% к десятому дню, что в основном гарантирует, что прогноз концентрации морского льда не отклонится более чем на один класс (20%) [11]. Это позволяет произвести точную локализацию границ льда, что ведет к снижению риска ложных прогнозов в навигационно-опасных зонах.

Машинное обучение доказало свою эффективность как инструмент повышения достоверности геоинформационных систем арктического мониторинга. Гибридные архитектуры решают фундаментальную проблему пространственно-временного анализа, обеспечивая снижение ошибки прогноза, увеличении пространственного разрешения и скорости вычислений в реальном времени (секунды против часов у физических моделей). Модели на основе LSTM показывают среднеквадратичную ошибку 8.89% для месячных прогнозов (среднегодовое значение), что соответствует снижению ошибки примерно на 28% по сравнению с традиционной авторегрессионной моделью (AR) [9].

Согласно Стратегии развития Арктической зоны РФ до 2035 года, к основным задачам в сфере защиты от чрезвычайных ситуаций относится развитие систем мониторинга обстановки и прогнозирования чрезвычайных ситуаций в Арктической зоне, в том числе на основе обработки данных дистанционного зондирования Земли из космоса [17]. Рассмотренные архитектуры глубокого обучения демонстрируют значительное превосходство над традиционными методами в точности и скорости прогнозирования. Для интеграции моделей машинного обучения в операционные системы навигационно-гидрографического обеспечения инфраструктуры СМП недостаточно достижения высоких метрик точности. Требуется обеспечить валидацию и воспроизводимость результатов, защиту от вычислительных артефактов, квантификацию неопределенности для информированного принятия решений, а также технологический суверенитет через разработку собственных архитектур машинного обучения на базе российских научных школ (ААНИИ, ИО РАН), собственных источников данных (например, Арктика-М, Метеор-М) и независимой вычислительной инфраструктуры.

#### СПИСОК ЛИТЕРАТУРЫ

1. Ананьева А. А. Навигация в Арктике. Спутниковые стратегии повышения безопасности на море // *Universum: технические науки*. 2024. № 2 (119).
2. Афанасьева Е. В. [и др.]. Методика составления ледовых карт ААНИИ // *Российская Арктика*. 2019. № 7.
4. Волков В. А. [и др.]. Система мониторинга ледовых условий применительно к задачам обеспечения геологоразведочных работ в арктических морях Геленджик, Россия, 2017.
5. Заболотских Е. В. [и др.]. Спутниковое микроволновое зондирование морского льда Арктики. Обзор // *Современные проблемы дистанционного зондирования Земли из космоса*. 2023. № 1 (20). С. 9–34.
6. Куватов В. И., Козьмовский Д. В., Шаталова Н. В. Потенциал Северного морского пути Арктической зоны России. Факторы и стратегия развития // *Интернет-журнал «НАУКОВЕДЕНИЕ»*. 2014. № 6 (6).
7. Aksenov Y. [и др.]. On the future navigability of Arctic sea routes: High-resolution projections of the Arctic Ocean and sea ice // *Marine Policy*. 2016. (75).
8. Andersson T. R. [и др.]. Seasonal Arctic sea ice forecasting with probabilistic deep learning // *Nature Communications*. 2021. № 1 (12). С. 5124.
9. Bushuk M. [и др.]. A Mechanism for the Arctic Sea Ice Spring Predictability Barrier // *Geophysical Research Letters*. 2020. № 13 (47).
10. Chi J., Kim H. Prediction of Arctic Sea Ice Concentration Using a Fully Data Driven Deep Neural Network // *Remote Sensing*. 2017. № 12 (9). С. 1305.
11. Ivanova N. [и др.]. Retrieval of Arctic Sea Ice Parameters by Satellite Passive Microwave Sensors: A Comparison of Eleven Sea Ice Concentration Algorithms // *IEEE Transactions on Geoscience and Remote Sensing*. 2014. № 11 (52). С. 7233–7246.
12. Liu Q. [и др.]. Daily Prediction of the Arctic Sea Ice Concentration Using Reanalysis Data Based on a Convolutional LSTM Network // *Journal of Marine Science and Engineering*. 2021. № 3 (9). С. 330.
13. Radhakrishnan K., Scott K., Clausi D. Sea Ice Concentration Estimation: Using Passive Microwave and SAR Data With a U-Net and Curriculum Learning // *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*. 2021. (PP). С. 1–1.
14. Ronneberger O., Fischer P., Brox T. U-Net: Convolutional Networks for Biomedical Image Segmentation // 2015.
15. Wei J., Hang R., Luo J.-J. Prediction of Pan-Arctic Sea Ice Using Attention-Based LSTM Neural Networks // *Frontiers in Marine Science*. 2022. (9).
16. *Proceedings of the Global AI Congress 2019* под ред. J. K. Mandal, S. Mukhopadhyay, Singapore: Springer Singapore, 2020.
17. Распоряжение Правительства Российской Федерации от 27 ноября 2021 года №3363-р «Об утверждении Транспортной стратегии Российской Федерации до 2030 года с прогнозом на период до 2035 года» [Электронный ресурс]. URL: <https://www.mintrans.gov.ru/file/473193> (дата обращения: 01.10.2024).
18. Стратегия развития Арктической зоны Российской Федерации и обеспечения национальной безопасности на период до 2035 года // Совет Безопасности Российской Федерации [Электронный ресурс]. URL: [http://www.scrf.gov.ru/security/economic/Arctic\\_strategy/](http://www.scrf.gov.ru/security/economic/Arctic_strategy/) (дата обращения: 05.10.2025).

УДК 004.94

#### ГЕОИНФОРМАЦИОННАЯ СИСТЕМА КАК ОСНОВА АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ОПТИМАЛЬНЫМ ФУНКЦИОНИРОВАНИЕМ ЭЛЕКТРОЭНЕРГЕТИЧЕСКОЙ СИСТЕМЫ В УСЛОВИЯХ ВОЗДЕЙСТВИЯ ЭКСТРЕМАЛЬНЫХ ПОГОДНЫХ ЯВЛЕНИЙ

Бурлов Вячеслав Георгиевич<sup>1</sup>, Полюхович Максим Алексеевич<sup>2</sup>, Логвинова Юлия Валерьевна<sup>2</sup>

<sup>1</sup> Российский государственный гидрометеорологический университет  
ул. Воронежская, 79, Санкт-Петербург, 192007, Россия

<sup>2</sup> Санкт-Петербургский политехнический университет Петра Великого  
ул. Политехническая, 29 лит. Б, Санкт-Петербург, 195251, Россия

e-mails: burlovvg@mail.ru, polyuhovich\_ma@spbstu.ru, logvinova\_yuv@spbstu.ru

**Аннотация.** Применён подход на основе синтеза для системной интеграции базовых процессов обеспечения безопасности критически важного объекта. Разработана модель автоматизированных систем управления, базирующаяся на технологиях геоинформационного моделирования, для оптимального функционирования электроэнергетической системы.

**Ключевые слова:** воздушные линии электропередачи; автоматизация; оптимизация; электроснабжение; природно-климатические условия.

# GEOINFORMATION SYSTEM AS AN AUTOMATED CONTROL SYSTEMS BASIS FOR ELECTRIC POWER SYSTEMS OPTIMAL FUNCTIONING UNDER CONDITIONS OF EXTREME WEATHER PHENOMENA IMPACT

Burlov Vyacheslav<sup>1</sup>, Polyukhovich Maxim<sup>2</sup>, Logvinova Yulia<sup>2</sup>

<sup>1</sup> Russian State Hydrometeorological University

79 Voronezhskaya str., St. Petersburg, 192007, Russia

<sup>2</sup> Peter the Great St. Petersburg Polytechnic University

29 B Polytechnicheskaya str., St. Petersburg, 195251, Russia

e-mails: burlovvg@mail.ru, polyuhovich\_ma@spbstu.ru, logvinova\_yuv@spbstu.ru

**Abstract.** A synthesis-based approach was applied to the system integration of basic safety processes at a critical facility. A model of automated control systems based on geoinformation modeling technologies was developed for the optimal operation of the electric power system.

**Keywords:** overhead power lines; automation; optimization; power supply; natural and climatic conditions.

Введение. Процесс устойчивого и надёжного развития страны усложнен тем, что воздействие природно-климатических факторов на процесс передачи электроэнергии неоднородно и вызывает кратковременные или долговременные перебои в электроснабжении. Такие перебои пагубно сказываются на государстве и населении, так как, во-первых, приводят к уменьшению экономических показателей в связи с остановкой функционирования промышленных предприятий, во-вторых, являются источником создания аварийных ситуаций, так как часть систем обеспечения безопасности и жизнеобеспечения зависят от бесперебойного электропитания.

Природно-климатические условия Российской Федерации уникальны, 28% территории относятся к Арктической зоне. Арктика характеризуется экстремальными погодными явлениями, такими как штормовой ветер, низкая температура, высокая влажность и т.д. В настоящее время идёт интенсивное освоение территории Арктической зоны, в связи с чем необходимо развивать инфраструктуру региона. Для этого, в первую очередь, необходимо проектировать, строить и в дальнейшем эксплуатировать объекты электроэнергетической системы.

Наиболее подверженным природно-климатическим факторам элементом системы электроснабжения являются воздушные линии электропередачи (ВЛЭП) [1]. Их ключевые особенности, такие как большая протяжённость проводов, размещение на открытой местности, подвижка грунтов под опорами линий электропередачи, обуславливают крайне низкую устойчивость ВЛЭП к факторам окружающей среды [2-3].

При проектировании ВЛЭП закладываются все необходимые условия для их длительного и безаварийного функционирования. Но в случае проявления экстремальных погодных явлений, как, например, на территории Арктики, реальная нагрузка превышает допустимую расчётную. Для своевременного и оперативного прогнозирования состояния ВЛЭП необходим инструмент, позволяющий в кратчайшие сроки достоверно охарактеризовать обстановку на наблюдаемой территории. При этом данный инструмент должен быть положен в основу автоматизированных систем управления (АСУ), чтобы исключить влияние человеческого фактора.

АСУ можно определить как область компьютерных наук, которая автоматизирует разумное поведение человека. В основе разумного поведения человека лежит его решение. Без методологии решения проблем функционирования АСУ как условия существования процесса нельзя гарантировать достижение цели деятельности – обеспечение устойчивого бесперебойного электроснабжения.

Цель исследования – для автоматизации процесса оценки состояния объекта (ВЛЭП) в условиях воздействия экстремальных погодных явлений разработать модель решения человека, базирующуюся на технологиях геоинформационного моделирования.

Применение естественно-научного подхода [4-5] позволяет для разработки модели решения человека использовать Закон сохранения целостности объекта (ЗСЦО) [6-7]. ЗСЦО – это устойчивая, объективная, повторяющаяся связь свойств объекта и свойств его действий при фиксированном предназначении.

В случае моделирования воздействия экстремальных погодных явлений на ВЛЭП необходимо иметь характеристики гидрометеорологических факторов (скорость ветра, значения температуры и влажности), а также описание наблюдаемого атмосферного явления (гроза, шторм, ливень и т.д.). Получить указанную информацию можно при помощи интенсивно развивающихся геоинформационных систем (ГИС), которые позволяют изучить данные о погодных условиях на определённый период.

В данном исследовании принимается, что человек воспринимает факты, упорядоченные во времени, в связи с этим охарактеризуем «Объект» («ВЛЭП») как среднее время проявления опасности возникновения предельно допустимой нагрузки от воздействия экстремального погодного явления, которая приводит к обрыву ВЛЭП и последующим перебоям в электроснабжении. Такую опасность обозначим в модели через  $\Delta t_{П}$ . Категорию «Действие» («Информационно-аналитическая работа в ГИС») в исследовании обозначим как среднее время идентификации предельно допустимой нагрузки, выразив через  $\Delta t_{ИП}$ . Категория «Предназначение» («Решение») выражается через среднее время нейтрализации перебоев в электроснабжении региона –  $\Delta t_{НП}$ . В рамках исследования предполагается, что указанные временные интервалы являются случайными величинами.

Для устранения возможных перерывов в электроснабжении необходимо синтезировать модель решения человека. Математическая модель позволит устанавливать временные параметры процессов идентификации и нейтрализации для достижения цели деятельности. Это повысит эффективность функционирования АСУ за счёт сокращения времени реагирования и внедрения превентивных мер.

Для этого на основании трёх компонентов: «ВЛЭП», «Информационно-аналитическая работа в ГИС», «Решение» разработаем математическую модель решения человека, используя последовательно методы декомпозиции, абстрагирования и агрегирования:  $P = f(\Delta t_{IP}, \Delta t_{II}, \Delta t_{NP})$ , где  $P$  – показатель эффективности автоматизированного управления безопасностью ВЛЭП на базе ГИС в условиях воздействия экстремальных погодных явлений.

**Заключение.** Таким образом, в качестве основы АСУ предложена модель решения человека, содержащая три базовых элемента: «ВЛЭП», «Информационно-аналитическая работа в ГИС», «Решение». Установив требуемый показатель эффективности автоматизированного управления безопасностью ВЛЭП, имеется возможность разработать комплекс мероприятий для предотвращения перебоев в электроснабжении при возникновении предельно-допустимой нагрузки на основе комбинации двух составляющих вектора управления:  $\Delta t_{II}$ ,  $\Delta t_{NP}$ .

Исследование выполнено при поддержке Министерства науки и высшего образования Российской Федерации в рамках соглашения № 075-15-2025-673 от 20.08.2025.

#### СПИСОК ЛИТЕРАТУРЫ

1. Харитонов Т.В. Использование цифровых датчиков обнаружения гололедных отложений на проводах линий электропередачи // Известия ТулГУ. Технические науки. 2023, №12. С. 487-489.
2. Бойкова Т.В. Качество и надежность энергосистем малой мощности // НиКСС. 2023, №3 (43). С. 28-37.
3. Лапина А.М. Причины повреждений линий электропередачи и методы их обнаружения // Auditorium. 2023, №2 (38). С. 87-91.
4. Бурлов В.Г. Основы теории синтеза облика системы обеспечения безопасности и способов ее функционирования на потенциально опасных объектах // Проблемы управления рисками в техносфере. 2012, № 3 (23). С. 1-13.
5. Бурлов В.Г. Моделирование процесса управления социальными и экономическими системами региона на основе потенциально активных элементов пространства и времени // Проблемы экономики и управления в торговле и промышленности. 2013, № 3 (3). С. 82-85.
6. Бурлов В.Г. Методологический подход к оценке безопасности функционирования социальной и экономической системы управления региона // Проблемы экономики и управления в торговле и промышленности. 2013, № 2 (2). С. 99-103.
7. Бурлов В.Г. Разработка модели управления процессами обеспечения безопасности эксплуатации электроустановки // Техно-технологические проблемы сервиса. 2018, № 4 (46). С. 33-38.

УДК 651.012.7

#### ГЕОКОНТРОЛЛИНГОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕРРИТОРИАЛЬНЫХ АКТИВНОСТЕЙ ПУБЛИЧНОЙ ВЛАСТИ В РЕГИОНЕ

**Бурлов Вячеслав Георгиевич<sup>1</sup>, Миронов Алексей Юрьевич<sup>2</sup>, Миронова Анна Юрьевна<sup>3</sup>**

<sup>1</sup> Государственный университет морского и речного флота имени адмирала С. О. Макарова,  
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия

<sup>2</sup> Российский государственный гидрометеорологический университет  
пр. Металлистов, 3, Санкт-Петербург, 195027, Россия

<sup>3</sup> Санкт-Петербургский политехнический университет Петра Великого,  
Политехническая ул. 29, Санкт-Петербург, 195251, Россия

e-mails: burlovvg@mail.ru, aperespelov@gmail.com, wakepolarbear@gmail.com, wakedeer@gmail.com

**Аннотация.** С целью эффективного исполнения законов РФ от 08.12.2020 № 394-ФЗ и от 21.12.2021 № 414-ФЗ рассматривается геоконтроллинг-поддержка информационной безопасности территориальных активностей исполнительной системы публичной власти в регионе. В качестве адекватного аппарата реализации на риск-ориентированных территориях предлагаются геоинформационная модель управляемой активности исполнительного органа, а также геоинформационный критерий оперативной оценки обстановки и выработки территориально-содержательных решений региональным активностям публичной власти.

**Ключевые слова:** публичная власть; территориальная активность; геоконтроллинг; оценка обстановки; управленческое решение; риск-ориентированная территория.

#### GEOCONTROLLING PROVISION FOR INFORMATION SECURITY OF TERRITORIAL /ACTIVITIES OF PUBLIC AUTHORITY IN THE REGION

**Burlov Vyacheslav<sup>1</sup>, Mironov Aleksey<sup>2</sup>, Mironova Anna<sup>3</sup>**

<sup>1</sup> Admiral Makarov State University of Maritime and Inland Shipping  
5/7 Dvinskaya St., St. Petersburg, 198035, Russia

<sup>2</sup> Russian State Hydrometeorological University  
3 Metalworkers Pr., St. Petersburg, 195027, Russia

<sup>3</sup> Peter the Great St. Petersburg Polytechnic University,  
29 Polytechnicheskaya St., St. Petersburg, 195251, Russia

e-mails: burlovvg@mail.ru, aperespelov@gmail.com, wakepolarbear@gmail.com, wakedeer@gmail.com

**Abstract.** In order to effectively enforce the laws of the Russian Federation No. 394-FZ dated 12/08/2020 and No. 414-FZ dated 12/21/2021, geocontrolling support for information security of territorial activities of the executive system of public authority in the region is being considered. As an adequate apparatus for implementation in risk-oriented territories, a geoinformation model of the managed activity of the executive body is proposed, as well as a geoinformation criterion for the operational assessment of the situation and the development of territorially meaningful decisions for regional activities of public authority.

**Keywords:** public authority; territorial activity; geocontrolling; situation assessment; management decision; risk-oriented territory.

В связи с поправкой в Конституцию РФ от 14.03.2020 № 1-ФКЗ, законами РФ от 08.12.2020 № 394-ФЗ и от 21.12.2021 № 414-ФЗ реализация публичной власти нацелена на наиболее эффективное решение государственных задач обеспечения устойчивости качества жизни населения, социально-экономического развития субъекта РФ. К повседневному предназначению территориальных активностей исполнительных органов публичной власти (ИОПВ) в регионе относится всестороннее, полное, объективное и оперативное выявление обстоятельств, причин и условий происшествий, пресечение проблем их негативного влияния на устойчивое развитие региона, минимизация и компенсация ущерба от них [1].

Характерными примерами пространственных происшествий, часто не выявляемых своевременно и создающих невосполнимый ущерб, являются:

- административные правонарушения подведомственности МВД, МЧС, ФСБ, Минприроды, Минтранса России, Роспотребнадзора, Ростехнадзора, Россельхознадзора, и других ИОПВ, в том числе несоблюдения требований (режима) охраны окружающей среды, наносящие вред экологии территорий; нарушения правил противопожарной безопасности, приводящее к площадным пожарам; незаконные вырубки леса, вылов рыбы, добыча диких животных и растений, нарушающие баланс и среду обитания биоресурсов; самовольные застройки, использование земель и добыча ископаемых, разрушающие территориальную систему природопользования; массовые драки и беспорядки, дестабилизирующие правопорядок.

- чрезвычайные ситуации природного или техногенного характера, в том числе природные пожары, наводнения, промышленные аварии, разрушения конструкций и строений;

- аварии на сетях, в том числе обрывы линий электропередач или связи, утечки из нефте-, газо- или бензопроводов, канализационных коллекторов, теплотрасс, водоводов, коммунальных систем;

- нарушения порядка на общественно-политических или спортивно-массовых мероприятиях;

- срывы плановых сроков национальных проектов или региональных программ развития территорий.

Факторы и параметры потоков пространственных происшествий носят явно выраженный территориальный характер, так как их объекты и субъекты располагаются и взаимодействуют в конкретных координатах земной поверхности (территории) с учетом ее особенностей [2]. Эффективность ИОПВ оценивается устойчивостью их территориальной активности, требующей неукоснительного соблюдения сроков при достаточном объеме процессуальных процедур за счет способности территориально локализовать пространственные происшествия, распознавать их латентность, вскрывать и преодолевать недобросовестные действия участников [3]. Обеспечение устойчивости в значительной мере зависит от наличия и качества располагаемой геоинформации о территориальных аспектах (о расположении, распространении, перемещении, взаимодействии, воздействии объектов и субъектов) проблемных происшествий, их выявления и пресечения, устранения ущерба от них.

Наряду с геоинформацией о территориальной активности, ИОПВ нуждаются в специальных методах обработки и преобразования мониторинговой геоинформации, оценки обстановки в регионе, ее опасностей и угроз, выработки рекомендаций по оптимизации своей территориальной активности, снижению рисков возникновения проблем и последствий от них [4]. Современные геоинформационные системы обеспечивают типовой спектр средств обработки и анализа геоинформации, ориентированный на выявление определенных признаков происшествий широким кругом различных пользователей. Реализации требований закона РФ от 21.12.2021 № 414-ФЗ о консолидации усилий и слаженности взаимодействия ИОПВ призвана способствовать геоинформационная поддержка информационной безопасности территориальных активностей в регионе [5].

Предлагаемые модель управляемой активности ИОПВ и критерий регулирования регионального управления ею базируются на методах системного и пространственного анализа, теории функциональных систем [6], теоретической геоинформатики, теории управления в пространстве состояний [7], формальной аксиоматической логики, структурно-функционального синтеза, математического и сетевого моделирования [8], теории марковских случайных процессов [9], теории вероятности [10]. Геоинформационная модель активности ИОПВ региона в потоке однородных происшествий отличается получением универсальных системообразующих зависимостей вероятностных характеристик состояний от интенсивностей управленческих процессов, определенных структурой и функциональностью на риск-ориентированных территориях, что гарантирует упреждающий контроль и поддержку достаточной устойчивости территориальной активности публичной власти. Геоинформационный критерий оперативной оценки обстановки и выработки территориально-содержательных рекомендаций по риск-ориентированному управлению региональными активностями публичной власти отличается корреляцией показателей устойчивости со структурой и функциональностью трех уровней территориально-содержательного регулирования: процедур внутри управленческих процессов, процессов



в подсистемах управления, подсистем в системе, что обеспечивает адекватный геоконтроллинг активностей ИОПВ региона с настройкой под достаточную устойчивость их управленческих процессов на риск-ориентированных территориях. Представленный модельно-методический аппарат геоконтроллинга способен адекватно отслеживать и поддерживать выше нормативного уровня (не менее 75%) устойчивость активностей ИОПВ в потоках однородных происшествий на риск-ориентированных территориях региона [11].

Таким образом, преодолевается противоречие между геоконтроллинговыми потребностями системы регионального управления территориальными активностями ИОПВ и отсутствием адекватных модельно-методических средств ее территориально-содержательного представления и регулирования. Исполнительная система публичной власти региона дополняется модельно-методическим аппаратом геоконтроллинга ее территориальной активности путем пространственной интерпретации категорий и процедур управления, придания контроллинговой динамики традиционному картографированию обстановки, что позволяет поддерживать устойчивость социально-экономического развития субъекта РФ информационной системой территориально-содержательного представления региональных активностей и регулирования системы регионального управления ими. Предлагаемые модель и критерий геоконтроллинга территориальных активностей публичной власти региона развивают в свете Указа Президента РФ от 18.06.2024 № 529 критические наукоемкие технологии создания программного обеспечения для управления социально и экономически значимой системой, мониторинга окружающей среды, предупреждения и снижения рисков чрезвычайных ситуаций природного и техногенного характера и негативных последствий.

#### СПИСОК ЛИТЕРАТУРЫ

1. Романчук И.С. Проблематика концепции публичной власти в субъектах Российской Федерации // Конституционное и муниципальное право. 2025, № 2. С. 40–44.
2. Грачев Н.И. Территориальная организация публичной власти. – М.: Юрайт, 2025. 471 с.
3. Ульянов А.Ю. Принцип эффективности и его место в современной российской парадигме публичной власти // Вестник Томского государственного университета. 2023, № 493. С. 228–235.
4. Биденко С.И., Самотонин Д.Н., Яшин А.И. Геоинформационные модели и методы поддержки управления. – СПб.: ФВУ ПВО, 2003. 224 с.
5. Бородин Е.Л., Звездарев Д.В., Биденко С.И., Милияков Д.Ф., Миронов А.Ю. Подходы к реализации геоконтроллинга морской транспортной деятельности в условиях киберспособности флота // Эксплуатация морского транспорта. 2025, №1(114). С. 56–62.
6. Анохин П.К. Принципиальные вопросы общей теории функциональных систем. – М.: Директ-Медиа, 2008. 131 с.
7. Филиповский В.М. Системы управления в пространстве состояний. – СПб.: СПбПУ, 2022. 75 с.
8. Катаргин Н.В., Невежин В.И. Сетевые модели в задачах экономики. – СПб.: Лань, 2020. 172 с.
9. Дворяткина С.Н., Проскуратова О.Н. Марковские процессы и простейшие модели теории массового обслуживания. – М.: ФЛИНТА, 2022. 90 с.
10. Положинцев, Б.И. Теория вероятностей и математическая статистика. – СПб.: СПбПУ, 2016. 95 с.
11. Бурлов В.Г., Переспелов А.В., Миронов А.Ю., Миронова А.Ю., Кадрян К.К. Моделирование риск-ориентированных целеуказаний для геоинформационного управления стадиями административного производства // Информация и космос. 2024, № 3. С. 102–110.

УДК 004.056:528.91

#### РАЗРАБОТКА МОДЕЛИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОПЕРАЦИОННОЙ СИСТЕМЫ В КОНТУРЕ УПРАВЛЕНИЯ ГЕОИНФОРМАЦИОННОЙ СИСТЕМОЙ

**Бурлов Вячеслав Георгиевич, Музалева Анна Юрьевна**

Российский государственный гидрометеорологический университет

Проспект Малоохтинский д. 98, Санкт-Петербург,

195196, Россия

e-mails: burlovvg@mail.ru, aniamuzaleva@yandex.ru

**Аннотация.** Работа посвящена разработке модели обеспечения безопасности операционной системы в контуре управления геоинформационной системой. Рассматриваются принципы построения аналитической динамической модели управления, основанной на законе сохранения целостности объекта и использовании Web-технологий.

**Ключевые слова:** геоинформационная система; безопасность; операционная система; модель управления; закон сохранения целостности объекта; Web-технологии; аналитическая динамическая модель; управление деятельностью.

#### DEVELOPMENT OF AN OPERATIONAL SYSTEM SECURITY MODEL IN A GEOINFORMATION SYSTEM MANAGEMENT CONTEXT

Burlov Vyacheslav, Muzaleva Anna

Russian State Hydrometeorological University

98 Malookhtinsky Avenue, Saint Petersburg, 195196, Russia

e-mails: burlovvg@mail.ru, aniamuzaleva@yandex.ru

**Abstract.** The work is devoted to the development of a model for ensuring the security of an operating system in the control loop of a geoinformation system. The principles of building an analytical dynamic control model based on the law of preserving the integrity of an object and the use of Web technologies are considered. The importance of using this approach to improve the efficiency and reliability of the geoinformation system, as well as to ensure the guaranteed achievement of its goals, is demonstrated.

**Keywords:** geoinformation system; security; operating system; management model; law of preserving object integrity; Web technologies; analytical dynamic model; and activity management.



Актуальность проблемы: существующие механизмы защиты операционных систем не учитывают специфику обработки пространственных данных в геоинформационных системах. Отсутствие специализированной модели безопасности создает угрозы целостности и конфиденциальности геоданных, что ведет к принятию неэффективных управленческих решений в сфере территориального планирования и госуправления.

Цель исследования: формулирование и обоснование аналитической динамической модели управления операционной системой в контуре геоинформационной системы (ГИС), обеспечивающей требуемый уровень безопасности, целостности и оперативности функционирования в условиях использования Web-инструментария.

Для достижения поставленной цели необходимо выполнить ряд задач, а именно проанализировать существующие подходы к моделированию и управлению геоинформационными системами, исследовать методы интеллектуального анализа данных, применимые в задачах мониторинга и прогнозирования внутри ГИС, реализовать возможности Web-технологий для оперативного контроля и управления процессами в режиме реального времени, разработать математическую модель управления операционной системой в контуре ГИС, основанную на принципах сохранения целостности объекта. В условиях цифровизации управления ГИС возрастает значение обеспечения безопасности и целостности их операционной среды. ГИС представляет собой сложный объект управления, функционирование которого зависит от согласованности процессов сбора, обработки и передачи пространственно-временных данных. Нарушение целостности хотя бы одного из элементов операционной системы может привести к деградации всей системы и потере управляемости.

Ключевым элементом эффективного управления является руководитель ГИС как лицо, принимающее решение (ЛПР). Его деятельность формируется на основе модели процесса управления. Однако традиционные аналитические подходы не позволяют гарантировать достижение цели деятельности в условиях динамически изменяющейся информационной среды.

Для решения данной проблемы применяется закон сохранения целостности объекта (ЗСЦО), формулирующий фундаментальное условие устойчивого функционирования любой управляемой системы. На основе ЗСЦО возможно синтезировать аналитическую динамическую модель решения руководителя, в которой процесс управления рассматривается как непрерывное преобразование состояния системы с сохранением её целостности.

Предлагаемая математическая модель управления операционной системой строится в рамках естественно-научного подхода (ЕНП), интегрирующего триаду «Мышление – Мир – Познание». Такой подход позволяет формализовать процесс принятия решений и описать взаимосвязи между управляющими воздействиями, параметрами состояния и целевыми функциями системы.

Использование Web-технологий в составе модели обеспечивает реализацию функций дистанционного контроля и оперативного управления. Это позволяет в режиме on-line отображать состояние всех технологических объектов геоинформационной системы, отслеживать изменение параметров и мгновенно принимать корректирующие решения.

Математическая основа модели представлена системой дифференциальных уравнений, описывающих динамику изменения состояний элементов операционной системы в процессе управления. Такой подход обеспечивает гарантированное достижение цели деятельности, поскольку система управления проектируется не на основе эмпирического анализа, а на основе синтеза, исходящего из фундаментального закона функционирования объекта.

Предложенный методологический подход формирует основу нового класса систем управления, в которых процессы обработки информации, принятия решений и реализации управляющих воздействий подчинены единому закону сохранения целостности объекта. Это позволяет перейти от реактивного к проактивному управлению, обеспечивая устойчивое развитие и безопасность функционирования геоинформационных систем в цифровой среде. Таким образом, результаты исследования подтверждают эффективность применения принципов синтеза моделей управления на основе естественно-научного подхода и закона сохранения целостности объекта. Предложенный метод обеспечивает переход от эмпирических к строго формализованным решениям, что является необходимым условием повышения надёжности и устойчивости геоинформационных систем в современной цифровой инфраструктуре.

## СПИСОК ЛИТЕРАТУРЫ

1. Орловский С. А. Проблемы принятия решений при нечеткой исходной информации. – М., 1981 – 206 с.
2. Анохин П.К. Системные механизмы высшей нервной деятельности. М. «Наука», 1979, 453 стр.
3. Burlov V.G., Grobtski A.M. Development of a Model for Social System Management in the Construction Process Taking into Account Manager's Qualification// Humanities & Science University Journal. №15 (2015), Peter the Great St. Petersburg Polytechnic University, Russia.2015, pp.25-36.
4. Запечников С.В. Обеспечение безопасности восстановительного резервирования информации в системах распределенного хранения данных – М.: МИФИ, 2005 –325с.
5. ВасильевР.М., ГончаровВ.Ю. Машинноеобучениеи анализданных. Учебник. —СПб.БХВ-Петербург,2022.
6. ЕмельяновВ.В., КурейчикВ.М., ЛейбушкинФ.Л. Методы оптимизации и в теории принятия решений. Учебник. —Москва: ИздательствоМГТУ имени Н.Э. Баумана, 2021.
7. АхметзяновА.Р., Карманов В.Г.Основы машинного обучения и анализа данных. Учебник. —Москва: УниверситетИТМО,2022.
8. ГорбачевВ.С., АндреевА.Н.Анализ временных рядов и прогнозирование. Учебник. —Москва: Академия,2022.
9. ПановА.В.Разработка управленческих решений: информационные технологии.М.:» ГорячаялинияТелеком», 2004.С.27-30.
10. Бурлов В.Г. О концепции гарантированного управления устойчивым развитием Арктической зоны на основе решения обратной задачи. // Информационные технологии и системы: управление, экономика, транспорт, право. 2015. № 2 (16). С. 99-111.
11. БоровиковВ.П.SPSS: искусство обработки информации. Анализ данных и подготовка отчетов. —Москва: Диалог-МИФИ,2020.
12. Фридман Дж.Х., Хастил Д., Тибширани Р. Обучение с учителем и непараметрическое оценивание. Перевод с английского. — Москва: Вильямс,2022.
13. КолесовЮ.Б., ПолянинаД.Анализ данных и прогнозирование.Учебник. —Москва: Высшаяшкола, 2021.
14. ДьяконовВ.П., КругловВ.В.МатлабиSimulink для радио инженеров. Учебное пособие. —Москва: Солон-пресс,2022.
15. ФроловаА.Б., ЩербакА.Ю.Информационнаябезопасностькомпьютерныхсистемисетей. Учебник. —Москва: Форум,2023.

УДК 004

**ГЕОИНФОРМАЦИОННЫЕ СИСТЕМЫ В МОДЕЛИ ПРИНЯТИЯ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ:  
СИСТЕМНЫЙ ПОДХОД НА ОСНОВЕ ЗАКОНА СОХРАНЕНИЯ ЦЕЛОСТНОСТИ ОБЪЕКТА****Грачев Михаил Иванович**

Санкт-Петербургский университет МВД России  
Летчика Пилутова д., 1, Санкт-Петербург, 198206, Россия  
e-mail: mig2500@mail.ru

**Аннотация.** В работе рассматривается методология интеграции геоинформационных систем (ГИС) в процесс принятия управленческих решений на основе закона сохранения целостности объекта. Предложена аналитико-динамическая модель решения лица принимающего решение (ЛПР), формализующая процесс обработки пространственной информации в условиях информационного противоборства. Модель основана на системном представлении трех базовых процессов: образования проблемы, ее идентификации и нейтрализации.

**Ключевые слова:** геоинформационные системы; модель принятия решений; закон сохранения целостности; информационная безопасность; системная интеграция; аналитико-динамическая модель.

**GEOINFORMATION SYSTEMS IN THE MANAGEMENT DECISION-MAKING MODEL  
ARE A SYSTEMATIC APPROACH BASED ON THE LAW OF PRESERVING  
THE INTEGRITY OF AN OBJECT****Grachev Mikhail**

Pilot Pilyutova Av, St. Petersburg, 198206, Russia  
e-mail: mig2500@mail.ru

**Abstract.** This paper examines a methodology for integrating geographic information systems (GIS) into management decision-making based on the law of conservation of object integrity. An analytical and dynamic model of decision-making is proposed, formalizing the process of processing spatial information in the context of information warfare. The model is based on a systemic representation of three basic processes: problem formation, identification, and neutralization.

**Keywords:** geographic information systems; decision-making model; integrity conservation law; information security; system integration; analytical-dynamic model.

Современные вызовы цифровой трансформации управления требуют принципиально новых подходов к организации процесса принятия решений. Геоинформационные системы, эволюционируя от инструмента картографии к комплексным аналитическим платформам, становятся основным элементом управленческой архитектуры. Однако интеграция ГИС в контур принятия стратегических решений порождает комплекс проблем информационной безопасности, требующих системного решения на основе синтеза управленческих теорий и технологий защиты информации [1].

Основа деятельности человека - решение, принимаемое на основе модели. Соответственно для преодоления возникающих проблем в информационной безопасности требуется модель решения ЛПР [2].

В условиях информационного противоборства целостность этой модели становится критическим фактором эффективности управления. Геоинформационные системы, аккумулируя пространственные данные, формируют модельное представление процессов, протекающих в социальных, экономических и технико-технологических системах [3].

Ключевой проблемой интеграции ГИС в процесс принятия решений является обеспечение адекватности модельного представления пространственных процессов в условиях воздействия угроз информационной безопасности. Постановка задачи включает:

1. Синтез адекватной модели решения ЛПР на основе закона сохранения целостности объекта;
2. Формализацию условий существования процесса управления с использованием ГИС;
3. Разработку механизма обеспечения информационной безопасности геопространственных данных.

В основе методологии лежит естественно-научный подход, реализующий принцип трехкомпонентности познания через категории «система», «модель» и «предназначение» [4].

Для синтеза модели решения ЛПР применяется закон сохранения целостности объекта, обеспечивающий системную интеграцию процессов обработки пространственной информации.

Процесс принятия решения формализуется через три взаимосвязанных компонента:

- обстановка (проблемное пространство);
- информационно-аналитическая работа;
- решение (условие реализации управления).

Аналитико-динамическая модель решения ЛПР представляется в виде агрегата, характеризующегося тремя временными интервалами:

- $\Delta t_{ПП}$  - среднее время проявления проблемы;
- $\Delta t_{ИП}$  - среднее время идентификации проблемы;
- $\Delta t_{НП}$  - среднее время нейтрализации проблемы.

Условие существования процесса управления имеет следующий вид:  $\Delta t_{ИП} + \Delta t_{НП} < \Delta t_{ПП}$ .

Система управления описывается четырьмя состояниями:

- A00 - проблема не идентифицирована и не нейтрализуется;
- A10 - проблема идентифицирована, но не нейтрализуется;
- A01 - проблема не идентифицирована, но нейтрализуется;
- A11 - проблема идентифицирована и нейтрализуется [5].

Динамика системы описывается системой дифференциальных уравнений Колмогорова-Чепмена. В стационарном режиме вероятность нахождения системы в состоянии A11 определяется соотношением:

$$P_{11} = (\lambda \times v_1 \times v_2) / [(\lambda + v_1)(\lambda + v_2)(v_1 + v_2)],$$

где  $\lambda$ ,  $v_1$ ,  $v_2$  - интенсивности переходов между состояниями:

- $\lambda$  – частота возникновения проблем в системе управления ГИС;
- $v_1$  – частота идентификации проблем возникающих в системе управления;
- $v_2$  – частота нейтрализации проблем возникающих в системе управления.

Интеграция аналитической динамической модели в геоинформационных системах позволяет применять разработанную модель, которая позволяет формализовать процесс принятия решений на основе ГИС через:

1. Информационную потребность - свойство личности, характеризующее отсутствие модельной интерпретации пространственных процессов;
2. Эффективность реализации - вероятность идентификации и нейтрализации пространственных проблем;
3. Фундаментальную ответственность - способность ЛПР решать целевые задачи в социально-экономической системе.

Условие гарантированного достижения цели управления в условиях информационного противоборства является то, что возникающие проблемы в системе управления ГИС идентифицируются и нейтрализуются в соответствии с требуемым показателем эффективности реализации решения получаемым на основе системообразующего фактора в основе которого лежит закон сохранения целостности объекта.

Предложенная аналитико-динамическая модель решения ЛПР на основе ГИС позволяет:

1. Обеспечить системную интеграцию процессов обработки пространственной информации
2. Формализовать условия существования процесса управления в условиях информационного противоборства;
3. Синтезировать адекватные модели принятия решений для социально-экономических систем.

Дальнейшие исследования должны быть направлены на разработку адаптивных механизмов защиты геопро пространственных данных на основе закона сохранения целостности объекта.

Разработанная аналитико-динамическая модель находит практическое применение при проектировании и эксплуатации геоинформационных систем. Рассмотрим основные направления реализации.

Современные ГИС должны обеспечивать целостность пространственных данных на всех этапах обработки. Архитектура такой системы включает:

- слой данных обеспечивает хранение и целостность геопро пространственной информации;
- аналитический слой реализует процессы идентификации и нейтрализации проблем;
- интерфейсный слой предоставляет средства визуализации и взаимодействия с ЛПР.

Критическим параметром архитектуры является соотношение:

$$t_{\text{обработки}} + t_{\text{реакции}} < t_{\text{развития угрозы}},$$

где  $t_{\text{обработки}}$  - время обработки пространственных данных,

$t_{\text{реакции}}$  - время принятия решения,

$t_{\text{развития угрозы}}$  - характерное время развития угрозы.

Для противодействия угрозам информационной безопасности в ГИС реализуется многоуровневая система защиты:

- защита целостности данных контроль пространственно-временной согласованности;
- обеспечение достоверности верификация источников геоданных;
- гарантированная доступность резервирование критических компонентов.

Вероятность успешного противодействия угрозам определяется выражением:

$$P_{\text{защиты}} = 1 - \prod (1 - P_i),$$

где  $P_i$  - вероятность нейтрализации  $i$ -й угрозы.

Рассмотрим практическое применение модели в системе мониторинга и прогнозирования чрезвычайных ситуаций (ЧС).

Параметры системы

- $\lambda = 0.1 \text{ ч}^{-1}$  (интенсивность возникновения ЧС);
- $v_1 = 0.8 \text{ ч}^{-1}$  (интенсивность идентификации угрозы);
- $v_2 = 0.6 \text{ ч}^{-1}$  (интенсивность нейтрализации угрозы).

Расчет эффективности системы. Вероятность успешного управления ЧС:

$$P_{11} = (0.1 \times 0.8 \times 0.6) / [(0.1 + 0.8)(0.1 + 0.6)(0.8 + 0.6)] \approx 0.72.$$

Оптимизация параметров. Для повышения эффективности системы до 0.95 требуется:

- увеличить  $v_1$  до  $1.2 \text{ ч}^{-1}$  (улучшение системы мониторинга);
- увеличить  $v_2$  до  $0.9 \text{ ч}^{-1}$  (оптимизация процедур реагирования).

Интеграция с системами искусственного интеллекта. Современные ГИС интегрируют алгоритмы искусственного интеллекта для повышения эффективности обработки пространственных данных.

Нейросетевые модели идентификации угроз. Глубокие нейронные сети позволяют автоматизировать процесс идентификации пространственных угроз:

- автоматическое распознавание объектов на космических снимках;
- выявление аномалий в пространственных данных;
- прогнозирование развития кризисных ситуаций.

Адаптивные системы поддержки принятия решений. Интеллектуальные системы на основе машинного обучения:

- адаптируют параметры модели под конкретную ситуацию;
- обучаются на исторических данных о принятии решений;
- предоставляют рекомендации по оптимизации управления.

Перспективы развития методологии. Разработка квантовых алгоритмов обработки геоданных.

Перспективным направлением является использование квантовых вычислений для:

- ускорения обработки больших объемов пространственных данных;
- решения сложных оптимизационных задач в реальном времени;
- повышения безопасности передачи геопропространственной информации.

Создание распределенных реестров пространственных данных. Технология блокчейн может обеспечить:

- неизменяемость истории изменений пространственных данных;
- децентрализованное хранение геоинформации;
- прозрачность процессов принятия решений.

Предложенная аналитико-динамическая модель принятия решений на основе ГИС демонстрирует высокую эффективность при решении задач управления в условиях неопределенности и противодействия. Ключевые результаты работы реализуются в разработке математической модели, формализующая процесс принятия решений в ГИС, определены условия существования устойчивого процесса управления, показана практическая реализуемость модели в системах мониторинга ЧС, обоснована эффективность интеграции с технологиями искусственного интеллекта.

Перспективные направления дальнейших исследований должны быть направлены для разработки адаптивных алгоритмов обучения моделей в реальном времени, создание квантово-устойчивых систем защиты геопропространственных данных, исследование применения модели в распределенных ГИС следующего поколения.

#### СПИСОК ЛИТЕРАТУРЫ

1. Бурлов В.Г. Основы моделирования социально-экономических и политических процессов. СПб: СПбПУ, 2017. 265 с.
2. Анохин П.К. Системные механизмы высшей нервной деятельности. М.: Наука, 1979. 453 с.
3. Грачев М.И., Бурлов В.Г. Аналитическо-динамическая модель управленческого решения в социально-экономических системах // Т-Comm: Телекоммуникации и транспорт. 2019. Т. 13. № 10. С. 27-34.
4. Mesarovic M.D., Takahara Ya. General Systems Theory: Mathematical Foundations. New York: Academic Press, 1975.
5. Бурлов В.Г., Грачев М.И. Системная интеграция процессов управления в условиях киберугроз // Информационная безопасность регионов России. 2020. С. 89-94.

УДК 004

#### ПРЯМАЯ И ОБРАТНАЯ ЗАДАЧА В ВОПРОСАХ УПРАВЛЕНИЯ ГЕОИНФОРМАЦИОННЫМИ СИСТЕМАМИ

Грачев Михаил Иванович

Санкт-Петербургский университет МВД России

Летчика Пилютова д., 1, Санкт-Петербург, 198206, Россия

e-mail: mig2500@mail.ru

**Аннотация.** Данная работа посвящена разработке и анализу математической модели, описывающей динамику функционирования геоинформационных систем в процессах управления территориальными объектами. Прямая задача позволяет оценить эффективность системы управления на основе заданных параметров функционирования. Обратная задача дает возможность определить оптимальные характеристики процессов управления, необходимые для достижения целевого уровня эффективности.

**Ключевые слова:** геоинформационные системы; прямая задача управления; математическая модель; обратная задача управления.

#### A DIRECT AND INVERSE PROBLEM IN THE MANAGEMENT OF GEOGRAPHIC INFORMATION SYSTEMS

Grachev Mikhail

Pilot Pilyutova Av, St. Petersburg, 198206, Russia

e-mail: mig2500@mail.ru

**Abstract.** This work is devoted to the development and analysis of a mathematical model describing the dynamics of the functioning of geographic information systems in the management of territorial objects. The direct task allows you

to evaluate the effectiveness of the control system based on the set operating parameters. The inverse problem makes it possible to determine the optimal characteristics of the management processes necessary to achieve the target level of efficiency.

**Keywords:** geographic information systems; direct control problem; mathematical model; inverse control problem.

В современных условиях цифровой трансформации геоинформационные системы (ГИС) становятся критически важным инструментом управления территориальными объектами и процессами. Эффективное использование ГИС требует создания комплексных моделей, позволяющих не только описывать текущее состояние системы, но и оптимизировать ее параметры для достижения целевых показателей.

Анализ существующих исследований показывает значительный интерес к проблемам управления ГИС. Работы Берлянт А.М. [1] посвящены фундаментальным вопросам геоинформационного картографирования и моделирования. Тикунов В.С. [2] рассматривает теоретические основы геоинформатики и методы пространственного анализа. Капралов Е.Г. [3] предлагает архитектурные решения для построения распределенных геоинформационных систем. Исследования Лурье И.К. [4] охватывают методы интеграции данных дистанционного зондирования Земли в ГИС, в то время как Стурман В.И. [5] разрабатывает методики пространственного анализа для решения прикладных задач.

Особый интерес представляют работы зарубежных авторов: Конеску Г. [6] исследует вопросы интеграции технологий дистанционного зондирования и ГИС, а Longley P.A. и соавторы [7] систематизируют принципы географических информационных наук. Современные аспекты управления большими пространственными данными нашли отражение в исследованиях Heywood I. [8] и De Smith M.J. [9].

Однако существующие подходы преимущественно ориентированы на решение прямой задачи оценки эффективности систем. В отличие от них, настоящее исследование сфокусировано на решении обратной задачи - определении требований к параметрам системы управления ГИС для достижения заданного уровня эффективности.

Для построения модели управления ГИС использован естественно-научный подход [10], который за счет декомпозиции, позволивший выделить три ключевых компонента:

- мониторинг пространственных объектов и процессов;
- анализ и идентификация проблемных ситуаций;
- принятие решений и нейтрализации проблем.

Формализация модели основана на временных характеристиках процессов:

- $\Delta t_{пп}$  - среднее время между проявлениями проблем в ГИС;
- $\Delta t_{ип}$  - среднее время идентификации проблем;
- $\Delta t_{нп}$  - среднее время нейтрализации проблем.

Математическая модель представлена в виде функциональной зависимости:  $P_2 = f(\Delta t_{пп}, \Delta t_{ип}, \Delta t_{нп})$ , где  $P_2$  – показатель того что все проблемы проявляющиеся в системе идентифицируются и нейтрализуются (показатель безопасности системы).

Динамика системы управления ГИС описывается графом состояний с четырьмя дискретными состояниями:

- S1 – состояние системы при штатном функционировании ГИС;
- S2 - состояние системы при успешном разрешении проблемной ситуации;
- S3 - состояние системы проявления проблемной ситуации;
- S4 - состояние системы идентификация проблемы.

Переходы между состояниями характеризуются интенсивностями:

- $\lambda = 1/\Delta t_{пп}$  - интенсивность возникновения проблем;
- $\nu_1 = 1/\Delta t_{ип}$  - интенсивность идентификации проблем;
- $\nu_2 = 1/\Delta t_{нп}$  - интенсивность нейтрализации проблем;

Динамика системы описывается системой дифференциальных уравнений Колмогорова:

$$dP_1/dt = -\lambda P_1 + \nu_2 P_4;$$

$$dP_2/dt = \nu_1 P_3 + \nu_2 P_4;$$

$$dP_3/dt = \lambda P_1 - \nu_1 P_3;$$

$$dP_4/dt = \nu_1 P_3 - \nu_2 P_4,$$

$$\text{где } P_1 + P_2 + P_3 + P_4 = 1.$$

При решении прямой задачи ведется анализ рассматриваемой системы управления ГИС. Для этого могут быть применены сетевые графики [11] и другие процессы планирования временного состояния рассматриваемой системы. По полученным критическим путям – наибольшему времени выполнения задачи управления, получаем время работы системы управления ГИС. Время, затрачиваемое на идентификацию и нейтрализации сбоев, угроз и проблем, которые возникают из-за различных внешних и внутренних факторов, влияющих на процесс управления. По полученным данным руководитель должен провести оценку состояния системы управления и предпринять действия к выработке решения на работу системы с эффективностью большей, чем в настоящее время. В связи, с чем возникает необходимость в решении обратной задачи для получения данных характеристик системы, позволяющих получить большую эффективность.

Ключевым преимуществом разработанной модели является возможность решения обратной задачи - определения требуемых параметров системы для достижения целевого значения вероятности успешного функционирования P2.

Для стационарного режима получено аналитическое выражение:  $P2 = (v1 \times v2) / [(\lambda + v1)(\lambda + v2)]$ .

Решение обратной задачи включает:

- задание целевого значения P2;
- определение допустимых диапазонов v1 и v2;
- нахождение оптимального соотношения параметров.

Полученным результатом решения обратной задачи будет являться известные параметры идентификации и нейтрализации проблемы возникающей в системе управления ГИС. Руководитель должен привлечь имеющиеся ресурсы (техническое оснащение и персонал) для достижения цели деятельности.

Соответственно для повышения v1 (идентификация проблем) необходимо:

- внедрение систем автоматического мониторинга;
- использование алгоритмов машинного обучения;
- развертывание распределенных сенсорных сетей.

Для увеличения v2 (нейтрализация проблем) необходимо:

- автоматизация процессов восстановления;
- создание резервных систем;
- разработка протоколов быстрого реагирования [12].

Пример расчета:

Исходные параметры:  $\lambda = 0.2$ ,  $v1 = 0.5$ ,  $v2 = 0.4$ ,  $P2 = (0.5 \times 0.4) / [(0.2 + 0.5)(0.2 + 0.4)] = 0.476$ .

Для достижения  $P2 = 0.7$  требуется:

- увеличить v1 до 0.8;
- увеличить v2 до 0.6.

Анализ показывает наличие эффекта насыщения при высоких значениях v1 и v2, что указывает на необходимость комплексного подхода к оптимизации системы.

Решение прямой и обратной задачи позволяет:

- оценить эффективность существующей системы управления ГИС;
- определить оптимальные параметры модернизации системы;
- обосновать инвестиции в развитие инфраструктуры;
- планировать мероприятия по повышению квалификации персонала.

Внедрение модели обеспечивает повышение надежности и эффективности управления геоинформационными системами за счет целенаправленной оптимизации ключевых параметров.

#### СПИСОК ЛИТЕРАТУРЫ

1. Берлянт А.М. Геоинформационное картографирование. М.: Аспект Пресс, 2020. 256 с.
2. Тикунов В.С. Геоинформатика. М.: Академия, 2018. 384 с.
3. Капралов Е.Г., Кошкарёв А.В., Тикунов В.С. Основы геоинформатики: в 2 кн. М.: Академия, 2021. 352 с.
4. Лурье И.К. Геоинформационное картографирование. Методы геоинформатики и цифровой обработки космических снимков. М.: КДУ, 2018. 424 с.
5. Стурман В.И. Пространственный анализ данных для экологов и географов. Ижевск: Удмуртский университет, 2017. 210 с.
6. Konecny G. Geoinformation: Remote Sensing, Photogrammetry and Geographic Information Systems. CRC Press, 2014. 416 p.
7. Longley P.A., Goodchild M.F., Maguire D.J., Rhind D.W. Geographic Information Science and Systems. Wiley, 2015. 477 p.
8. Heywood I., Cornelius S., Carver S. An Introduction to Geographical Information Systems. Pearson Education, 2011. 446 p.
9. De Smith M.J., Goodchild M.F., Longley P.A. Geospatial Analysis: A Comprehensive Guide to Principles, Techniques and Software Tools. Troubador Publishing, 2018. 516 p.
10. Бурлов, В. Г. Аналитическо-динамическая модель управленческого решения в социально-экономических системах на примере руководителя учебного заведения высшего образования / В. Г. Бурлов, М. И. Грачев // Т-Comm: Телекоммуникации и транспорт. – 2019. – Т. 13, № 10. – С. 27-34. – DOI 10.24411/2072-8735-2018-10314. – EDN SNJZQR.
11. Бурлов, В. Г. Применение сетевых моделей в социальных и экономических системах / В. Г. Бурлов, М. И. Грачев // Т-Comm: Телекоммуникации и транспорт. – 2021. – Т. 15, № 2. – С. 33-38. – DOI 10.36724/2072-8735-2021-15-2-33-38.
12. Грачев, М. И. Процессы принятия управленческих решений в образовательной организации на основе модели решения / М. И. Грачев, В. Г. Бурлов // Т-Comm: Телекоммуникации и транспорт. – 2025. – Т. 19, № 6. – С. 25-32. – DOI 10.36724/2072-8735-2025-19-6-25-32.

УДК 004

#### ПРОБЛЕМЫ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ И МЕТОДЫ ИХ РЕШЕНИЯ

Грачев Михаил Иванович

Санкт-Петербургский университет МВД России

Летчика Пилотова д., 1, Санкт-Петербург, 198206, Россия

e-mail: mig2500@mail.ru

**Аннотация.** В статье проведен системный анализ проблем, препятствующих эффективному применению геоинформационных систем (ГИС) в задачах территориального управления и принятия решений. Выявлены и классифицированы ключевые вызовы, относящиеся к технической инфраструктуре, качеству пространственных данных и человеческому фактору.

**Ключевые слова:** геоинформационные системы; проблемы ГИС; качество данных; производительность; человеческий фактор; оптимизация; управление данными.

## PROBLEMS OF GEOINFORMATION SYSTEMS AND METHODS OF THEIR SOLUTION

**Grachev Mikhail**

Pilot Pilyutova Av, St. Petersburg, 198206, Russia

e-mail: mig2500@mail.ru

**Abstract.** The article provides a systematic analysis of the problems that hinder the effective use of geographic information systems (GIS) in the tasks of territorial management and decision-making. Key challenges related to technical infrastructure, spatial data quality, and human factors have been identified and classified.

**Keywords:** geographic information systems; GIS problems; data quality; performance; human factor; optimization; data management.

Широкое внедрение геоинформационных технологий сталкивается с рядом системных проблем, которые снижают их эффективность и ограничивают потенциал в поддержке принятия решений [1].

Несмотря на мощный аналитический функционал современных ГИС, их практическая отдача напрямую зависит от корректности технической реализации, качества исходных данных и уровня подготовки пользователей. В данной статье проводится структуризация этих проблем и предлагаются пути их решения.

Классификация проблем ГИС и методы их решения. Анализ позволяет выделить три фундаментальные категории проблем. В первую группу входят технические и архитектурные проблемы. Данная группа проблем связана с аппаратно-программной основой ГИС. Низкая производительность и медленный отклик могут проявляться в связи с ростом объема информационного потока и следствием старого оборудования, в комплексе выдающего снижение эффективности работы его в целом. Другой причиной может служить обработка больших объемов данных, выполнении сложных пространственных запросов или визуализации детализированных карт. Это связано с недостаточными вычислительными ресурсами, неоптимизированной архитектурой сервера базы данных или сетевых задержек [2].

Данная проблема может быть решена через, проведение аппаратного апгрейда, оптимизации индексов пространственной базы данных, использование кэширования файлов карт, переход на облачные вычисления с масштабируемыми ресурсами, но тут нужно соизмерять с финансовыми возможностями предприятия.

Проблемы интеграции и несовместимости возникают при необходимости объединения данных из разнородных источников (веб-сервисы, CAD-файлы, табличные данные) с различными системами координат и форматами. Решением данной проблемы может быть разработка и внедрение процессов (извлечение, трансформация, загрузка) для нормализации данных, использование стандартизированных форматов позволяющих проводить расшифровку и интеграцию процессов применения промежуточного программного обеспечения (мидлваров).

Проблемы качества и доступности данных. Эта категория является одной из наиболее критичных, так как выводы, полученные из некачественных данных, не имеют ценности. Низкое качество данных включает неточность геопривязки, семантические ошибки, дублирование записей, неполноту атрибутивной информации, что приводит к срыву выполнения требующейся задачи и трате временного ресурса. Решением в данной ситуации может быть внедрение строгого цикла управления данными, включая валидацию, очистку (дедубликацию) и верификацию данных на этапе их поступления в систему. Использование автоматизированных инструментов контроля качества.

Другая проблема это неактуальность и недостаточность данных. Информация устаревает или не покрывает все необходимые для анализа объекты и атрибуты. Решением данной проблемы может стать подключение к официальным и верифицированным источникам (например, государственным кадастрам, данным), настройка процессов регулярного обновления, в том числе с привлечением краудсорсинговых платформ. Внешние факторы воздействия на предприятия могут нести угрозу, которая будет препятствовать их нормальному функционированию для решения данной проблемы можно использовать информационные интеллектуальные системы [3].

Организационные проблемы и проблемы, связанные с человеческим фактором. Данные проблемы обусловлены недостатками в управлении и подготовке пользователей. Дефицит компетенций у пользователей. Сотрудники не обладают достаточными навыками для работы со сложным ГИС-функционалом, что приводит к неполному использованию возможностей системы или ошибкам в интерпретации результатов [4].

Разработка и реализация программ постоянного обучения и повышения квалификации. Создание внутренней базы знаний и инструкций может стать решением данной проблемы.

Сложность интерфейса и функционала. Перегруженный и не интуитивный интерфейс создает высокий порог входа и снижает производительность труда. Решение: внедрение принципов юзабилити и User Experience (UX) при проектировании интерфейса, что решает задачу создания продукта, который является удобным, интуитивно понятным и эффективно удовлетворяет потребности пользователей, что достигается за счет исследования, структурирования, прототипирования и тестирования. Создание ролевых рабочих мест с настроенным под конкретные задачи интерфейсом, скрывающим нерелевантный функционал.

Неэффективное управление доступом. Неправильно настроенные роли и права могут, как ограничивать доступ к необходимым данным, так и позволять несанкционированное изменение критической информации. Решением может стать внедрение системы ролевого управления доступом, проведение регулярного аудита прав доступа [5].

Как итог необходимо отметить, что проблемы в области ГИС носят комплексный характер и требуют целостного, системного подхода к их решению. Недостаточно просто обновить серверное оборудование или закупить новое программное обеспечение. Эффективное функционирование геоинформационной системы возможно только при одновременном и сбалансированном решении технических, информационных и кадровых задач. Предложенная классификация и соответствующие методы позволяют сформулировать стратегический план по развитию ГИС-инфраструктуры, направленный на превращение ее в надежный и эффективный инструмент поддержки принятия управленческих решений.

Для снижения расходов связанных с требующимися изменениями в области ГИС-технологий может быть применено имитационное моделирование для получения предварительных статистических данных позволяющих проводить оценку целесообразности затрачиваемых финансовых средств на требующуюся модернизацию [6].

#### СПИСОК ЛИТЕРАТУРЫ

1. Скворцов, И. П. О проблеме человеческого фактора в обеспечении информационной безопасности / И. П. Скворцов, А. О. Титарев // Воздушно-космические силы. Теория и практика. – 2022. – № 23. – С. 106-113.
2. Трошин, Д. В. Безопасность предприятия: смысл, онтология, оценка / Д. В. Трошин. – Тверь: ТвГУ, 2015. – 212 с.
3. Золотова, В. А. Направления развития интеллектуальной информационной технологии прогнозирования состояния предприятий промышленности России в условиях неблагоприятных внешних воздействий / В. А. Золотова – 2022. – № 4(86). – С. 71-78.
4. Грачев, М. И. Математическая модель для принятия решений по противодействию киберугрозам в производстве / М. И. Грачев, В. Г. Бурлов // Информационные технологии в проектировании и производстве. – 2022. – № 4(188). – С. 22-27.
5. Бурлов, В. Г. О необходимости подготовки и переподготовки кадров в сфере безопасности информационных технологий / В. Г. Бурлов, М. И. Грачев, А. И. Примакин // ИБРР-2017. – СПб., 2017. – С. 470-472.
6. Грачев, М. И. Имитационное моделирование процессов управления / М. И. Грачев // Интеллектуальные системы в производстве. – 2022. – Т. 20, № 4. – С. 64-71.

УДК 004.056.5+004.62:528.8

#### МОДЕЛЬ ИНТЕГРАЦИИ ГЕОДАНЫХ В OSINT

**Грызунов Виталий Владимирович**

Санкт-Петербургский университет ГПС МЧС России  
Московский пр., 149, Санкт-Петербург, 196105, Россия  
e-mail: viv1313r@mail.ru

**Аннотация.** Предложена формальная модель интеграции геоданных в OSINT через граф знаний, где геоатрибуты выступают векторами логического вывода к конфиденциальной информации

**Ключевые слова:** OSINT; геоданные; геолокация; граф знаний; скрытый канал вывода; триангуляция; модель нарушителя; цифровой след; информационная безопасность; Blue Team.

#### A MODEL FOR INTEGRATING GEOSPATIAL DATA INTO OSINT

**Gryzunov Vitaly**

Federal State Budgetary Educational Institution of Higher Education "St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia"  
Army General E.N. Zinichev»  
149 Moskovsky Av, St. Petersburg, 196105, Russia  
e-mail: viv1313r@mail.ru

**Abstract.** A formal model for integrating geospatial data into OSINT is proposed, based on a knowledge graph in which geo-attributes serve as inference vectors leading to confidential information.

**Keywords:** OSINT; geospatial data; geolocation; knowledge graph; inference covert channel; triangulation; attacker model; digital footprint; information security; Blue Team.

#### 1. Введение: геоданные как особый класс открытых свойств

Геопространственные данные (геотеги, координаты, картографические метки) представляют собой мощный и уязвимый класс открытых свойств в OSINT. В отличие от традиционных атрибутов (email, никнейм), геоданные обладают уникальной способностью связывать цифровую идентичность с физическим местоположением. Эта особенность делает их критически важными как для атакующих, так и для защитников. Однако их интеграция в OSINT-процесс требует формализованной модели, учитывающей как семантические связи, так и ресурсные ограничения аналитика.

Важно отметить, что устойчивость геоинформационных систем (ГИС) к внешним воздействиям напрямую влияет на надёжность геоданных: как показано в работе [1], даже небольшие дестабилизирующие факторы могут существенно снижать «полезность» ГИС для конечного потребителя, что актуально и для OSINT-аналитики.

Основные положения:

#### 2. Формализация геоданных в рамках модели OSINT-нарушителя



Согласно формальной модели OSINT-нарушителя, геоданные рассматриваются как элементы множества свойств  $X$  :

- Геоатрибуты (например, GPS-coordinates, address) входят в универсальное множество атрибутов  $A$  ;
- Конкретные значения (например, <GPS-coordinates, 59.9386, 30.3141>) — это свойства  $x \in X$  ;
- Публичные геосвойства ( $X^{\text{pub\_geo}} \subseteq X^{\text{pub}}$ ) могут быть связаны с конфиденциальными свойствами ( $X^{\text{conf}}$ )

через специфические отношения  $r \in R_A$ , такие как:

- $r_{\text{metadata}}$ : изображение  $\rightarrow$  GPS-координата;
- $r_{\text{map\_match}}$ : координата  $\rightarrow$  адрес/объект инфраструктуры;
- $r_{\text{social\_geo}}$ : пост в соцсети  $\rightarrow$  геотег  $\rightarrow$  организация.

Эти связи формируют «скрытый канал вывода», нарушающий принципы мандатных моделей безопасности, что особенно опасно в системах критического применения, где доверие к источникам должно быть строго формализовано [2].

### 3. Геопространственные предикаты как часть инструментария OSINT-аналитика

В рамках формальной модели инструментарий аналитика  $P$  расширяется геоспецифическими предикатами:

- $\text{Pexif}(x, y)$ : файл  $x$  содержит в EXIF-данных координаты  $y$  ;
- $\text{Preverse\_geo}(y, z)$ : координаты  $y$  соответствуют адресу  $z$  ;
- $\text{Psatellite\_match}(y, w)$ : спутниковое изображение подтверждает наличие объекта  $w$  по координатам  $y$  .

Эти предикаты порождают отношения  $r \in R_A$ , которые становятся рёбрами в графе знаний  $G$ . Как показано в [1], эффективность таких связей в условиях дестабилизирующих факторов (например, искажение координат, устаревшие карты) требует введения интегральных и дифференциальных показателей адаптивности ГИС — что может быть перенесено в OSINT для оценки надёжности геовыводов.

### 4. Геолокация как путь в графе знаний: от цифрового следа к физическому объекту

Задача геоинтеграции в OSINT формализуется как поиск пути:

$$y_{\text{start}} \rightarrow r_1 \rightarrow y_1 \rightarrow r_2 \rightarrow \dots \rightarrow r_n \rightarrow x_{\text{c\_geo}},$$

где  $y_{\text{start}} \in Y_{\text{known}}$  — начальное публичное свойство (например, фото в Telegram), а  $x_{\text{c\_geo}} \in X^{\text{conf}}$  — конфиденциальное геосвойство (например, домашний адрес).

Такой путь может включать как прямые связи ( $\text{EXIF} \rightarrow$  координаты), так и многошаговые выводы (координаты  $\rightarrow$  здание  $\rightarrow$  организация  $\rightarrow$  ФИО). Важно, что даже при отсутствии прямого вторжения в систему, злоумышленник может восстановить конфиденциальную информацию — аналогично тому, как социальный инженер управляет «объектом связи» через обратную связь, формализованную в терминах теории управления [3].

### 5. Триангуляция геоданных и независимость источников

Достоверность геовывода повышается при наличии независимых путей к одному и тому же геообъекту. Согласно модели OSINT-нарушителя, источники считаются независимыми, если их пути в графе не пересекаются по промежуточным узлам и рёбрам. Это позволяет формализовать геопространственную триангуляцию как пересечение образов независимых отношений.

Подход использует методы структурно-функционального синтеза, применяемые при построении систем обнаружения вторжений [4], где комбинирование независимых индикаторов повышает точность детекции.

### 6. Риски и угрозы: геоданные как «скрытый канал вывода»

Геоинформация часто публикуется легально (например, сотрудник делится фото с работы) и в совокупности с другими открытыми данными создаёт скрытый канал вывода, нарушающий принципы мандатных моделей (в т.ч. Белла–Лападулы).

Пример:

- Публичный пост с фото офиса  $\rightarrow$  EXIF  $\rightarrow$  координаты  $\rightarrow$  идентификация секретного филиала.

Это демонстрирует, что угроза исходит не от утечки, а от логического вывода на основе связей, что требует управления не только данными, но и отношениями между ними — особенно в критически важных системах, где доверие к источникам должно быть строго верифицировано [2].

### 7. Фреймворк защиты: управление геопространственным цифровым следом

На основе модели Blue Team Playbook предложены меры:

- Аудит геоследа: сканирование публичных ресурсов на наличие геотегов, EXIF, картографических упоминаний;
- Разрыв геосвязей: очистка метаданных, отключение геолокации в корпоративных аккаунтах;
- Зашумление: публикация ложных геометок или использование общих координат (офис вместо дома);
- Мониторинг: автоматизированный контроль новых геотечек через API карт и соцсетей.

Эти действия направлены на снижение «полезности» геоданных для атакующего, что напрямую связано с концепцией адаптивности ГИС к дестабилизирующим факторам [1].

### 8. Заключение: геоданные как неотъемлемый элемент формальной OSINT-модели

Интеграция геоинформации в OSINT требует не просто инструментов, а формального понимания её роли в графе знаний. Предложенная модель позволяет:

- строго описывать геопространственные атаки;

- количественно оценивать риски через функцию останова  $F_{stop}$  ;
- проектировать защиту на основе разрыва опасных отношений  $r \in R_{pub} \rightarrow conf$ .

Это делает геоданные не просто «ещё одним источником», а ключевым вектором логического вывода в современных OSINT-угрозах — особенно в контексте защиты критической инфраструктуры, где вопросы доверия, адаптивности и устойчивости к дестабилизации требуют междисциплинарного подхода [4].

#### СПИСОК ЛИТЕРАТУРЫ

1. Burlov V. G., Gryzunov V. V. Evaluation of the effectiveness of geographic information systems adaptation to destabilizing factors // Journal of Physics: Conference Series. – 2020. – P. 012016.
2. Грызунов В. В., Корниенко А. А., Глухарев М. Л., Крюков А. С. Выбор моделей доверия при интеграции распределенных информационных систем критического применения // Проблемы информационной безопасности. Компьютерные системы. – 2021. – № 4. – С. 79–90.
3. Gryzunov V. V., Bondarenko I. Y. A Social Engineer in Terms of Control Theory // Proceedings of the 3rd International Conference Ergo-2018. – 2018. – P. 202–204.
4. Грызунов В. В. Структурно-функциональный синтез модели системы предотвращения вторжений // Проблемы информационной безопасности. Компьютерные системы. – 2006. – № 2. – С. 31–38

УДК 004.89

#### УЯЗВИМОСТИ В УПРАВЛЕНИИ МОДЕЛЯМИ МАШИННОГО ОБУЧЕНИЯ В ГЕОИНФОРМАЦИОННЫХ СИСТЕМАХ

**Колбина Ольга Николаевна, Служева Маргарита Ивановна, Микulyаева Анастасия Алексеевна**

Российский государственный гидрометеорологический институт,

Малоохтинский пр., 98, г. Санкт-Петербург, 195196, Россия

e-mails: olya\_kolbina@mail.ru, msluzheva@mail.ru, amikulyaeva@gmail.com

**Аннотация.** В данном исследовании рассматриваются этапы цикла управления моделями машинного обучения. Их управление с учетом ГИС. Описаны основные категории уязвимостей при внедрении и управлении моделями машинного обучения в ГИС. Приведены возможные рекомендации по их устранению.

**Ключевые слова:** уязвимости; машинное обучение; ГИС; управление моделями; географические данные.

#### VULNERABILITIES IN MACHINE LEARNING MANAGEMENT IN GEOGRAPHIC INFORMATION SYSTEMS

**Kolbina Olga, Sluzheva Margarita, Mikulyaeva Anastasia**

Russian State Hydrometeorological Institute, 98 Malookhtinsky Pr., St. Petersburg, 195196, Russia

e-mails: olya\_kolbina@mail.ru, msluzheva@mail.ru, amikulyaeva@gmail.com

**Abstract.** This study examines the stages of the machine learning model management cycle. Their GIS-based management. The main categories of vulnerabilities in the implementation and management of machine learning models in GIS are described. Possible recommendations for their elimination are provided.

**Keywords:** vulnerabilities; machine learning; GIS; model management; geographic data/

На сегодняшний день геоинформационные системы активно интегрируют модели машинного обучения (далее модели МО). В данном исследовании [1] показывается, как происходит анализ и обработка географических данных с помощью моделей МО, например, распознаются объекты на карте, прогнозируются пожары, рассчитывается оптимальное расположение инфраструктуры и другое. Однако, как отмечается в [2], такие модели подвержены ряду уязвимостей, включая смещения данных, атаки на этапе обучения и эксплуатации, а также ошибки при их интерпретации, что в контексте ГИС может привести к компрометации данных, снижению точности прогнозов, подделке пространственных выводов через атаки искажения или нарушению работы инфраструктурных систем. [3]. Данная проблематика обусловлена еще и растущим применением ГИС в государственном секторе [4], а также в мониторинге окружающей среды [5].

Цикл управления моделями МО состоит из нескольких этапов. Сначала определяют задачу для модели, далее собираются данные и преобразовываются, разделяются, после происходит выбор модели и обучения (например, модель - линейная регрессия, обучение - настройка гиперпараметров), следующим пунктом идет проверка модели на валидационной выборке и тонкая настройка параметров, потом оценка на тестовых данных (например, точность, устойчивость к выбросам и крайним случаям), развертывание и интеграция с другими системами, последними этапами являются мониторинг и обновление (то есть корректировка при необходимости) [6].

В ГИС модели МО начинают обучать уже по специальным данным [1]. Например, как менять характеристики объекта в разные сезоны года. После интеграции в ГИС производят оценку и оптимизацию различных метрик, которые имеют практическую применимость. Например, насколько важен объект ошибки, его площадь, влияние на экосистему. Далее происходят классические этапы, упомянутые выше, для цикла управления моделями МО.

Основные категории уязвимостей, которые могут быть в ГИС:

1. Первая группа уязвимостей связана с безопасностью обучающих данных [7]. Геопространственные данные часто агрегируются из множества источников различной степени надежности, что создает возможности для атак, связанных с искажением данных. Злоумышленник может внедрить такие образцы в обучающую выборку. Например, подмена нескольких эталонных точек при обучении модели классификации землепользования может привести к неверной идентификации промышленных зон как жилых.

2. Вторая категория уязвимостей касается защиты самих моделей. Модели МО в ГИС часто развертываются в распределенных средах с ограниченным контролем безопасности. Если отсутствует шифрование параметров модели [8], то, например, через адверсарные атаки можно манипулировать входными данными. Для ГИС это может означать изменения в спектральных характеристиках спутникового снимка, приводящие к ошибочной классификации объектов.

3. Третья область уязвимостей затрагивает процессы управления версиями и развертывания. Одну из опасностей представляют какие-либо изменения в моделях без системы их отслеживания в документацию. Использование устаревших моделей или, наоборот, обновление производственных моделей без должного тестирования может привести к непредсказуемым результатам в ГИС.

4. Четвертая группа связана с уязвимостями работы моделей МО в ГИС. Например, логирование предсказаний модели без надлежащей анонимизации может привести к утечке конфиденциальной геопространственной информации, раскрывающей персональные данные пользователей [7].

Эффективное управление моделями МО в ГИС предполагает комплексное обеспечение их надежности и безопасности на всех этапах жизненного цикла. Уязвимости могут возникать как на стадии подготовки и обучения данных, так и при развертывании и эксплуатации моделей. Для минимизации рисков рекомендуется осуществлять верификацию источников геоданных, использовать механизмы шифрования и многофакторной аутентификации при доступе к моделям, внедрять систему контроля версий и аудита изменений, а также регулярно проводить тестирование на устойчивость к адверсарным воздействиям. Реализация указанных мер способствует повышению достоверности результатов анализа и устойчивости ГИС к потенциальным угрозам.

#### СПИСОК ЛИТЕРАТУРЫ

1. Аманкулова Н. А., Молмакова М. С., Каримова Г. Т. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ГЕОИНФОРМАЦИОННЫЕ СИСТЕМЫ // Бюллетень науки и практики. 2023. №11.
1. Шанкар С. С., О'Брайен Д., Сновер Дж., Альберт К., Вилжоен С. Режимы сбоя в машинном обучении / Microsoft Corporation; Berkman Klein Center for Internet and Society at Harvard University. — 12 марта 2019 г. — URL: <https://learn.microsoft.com/ru-ru/security/engineering/failure-modes-in-machine-learning> (дата обращения: 05.10.2025)
2. Жасмин Ландресс, Сэмюэль Абеду, Ахмад Абделлатиф и Эмад Шихаб. 2024. Исследовательское исследование управления моделью машинного обучения. ACM Trans. Мягкий Англ. Метод. 34, 1, статья 16 (январь 2025 г.), 31 страница.
3. Ляхова Наталия Ивановна РАЗВИТИЕ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ В ИНФРАСТРУКТУРЕ ПРОСТРАНСТВЕННЫХ ДАННЫХ РОССИИ // РЭиУ. 2022. №4 (72).
4. Евдокимов Сергей Игоревич, Штефуряк Алина Викторовна ИСПОЛЬЗОВАНИЕ ГИС-ТЕХНОЛОГИЙ В МОНИТОРИНГЕ ПРИРОДНЫХ И АНТРОПОГЕННЫХ ОБЪЕКТОВ // Вестник Псковского государственного университета. Серия: Естественные и физико-математические науки. 2022. №1.
5. Основы машинного обучения: задачи, методы, этапы и инструменты / Yandex.Cloud. — 27 августа 2025 г. — URL: <https://yandex.cloud/ru-kz/blog/machine-learning-guide> (дата обращения: 05.10.2025)
6. NIX Solutions. Предложения относительно уязвимостей и защиты моделей машинного обучения / Habr. — 05 июля 2019 г. — URL: <https://habr.com/ru/companies/nix/articles/458892/> (дата обращения: 05.10.2025)
7. Чекмарев М. А., Ключев С. Г., Шадский В. В. МОДЕЛИРОВАНИЕ НАРУШЕНИЙ БЕЗОПАСНОСТИ В СИСТЕМАХ МАШИННОГО ОБУЧЕНИЯ // Научно-технический вестник информационных технологий, механики и оптики. 2021. №4.

УДК 004.89

#### РАЗРАБОТКА АЛГОРИТМОВ ДЛЯ КВАНТОВЫХ БАЗ ДАННЫХ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Колбина Ольга Николаевна, Фатин Дмитрий Романович, Федосеева Яна Артёмовна**

Российский государственный гидрометеорологический университет

195196, Россия, Санкт-Петербург, проспект Metallistov, д. 3, лит. А

e-mails: [olya\\_kolbina@mail.ru](mailto:olya_kolbina@mail.ru), [yanafedoseeva06@gmail.com](mailto:yanafedoseeva06@gmail.com), [mr.fatin2017@gmail.com](mailto:mr.fatin2017@gmail.com)

**Аннотация.** Рассматриваются методы защиты квантовых баз данных и перспективы их использования для усиления криптографических систем в условиях развития квантовых вычислений.

**Ключевые слова:** квантовые базы данных; квантовые алгоритмы; алгоритм Гровера; кибербезопасность; квантовая информационная безопасность.

#### DEVELOPMENT OF ALGORITHMS FOR QUANTUM DATABASES IN INFORMATION SECURITY

**Kolbina Olga, Fatin Dmitry, Fedoseeva Yana**

The Russia State Hydrometeorological University

195196, Russia, St. Petersburg, Metallistov Avenue, Building 3, Lit. A

e-mails: [olya\\_kolbina@mail.ru](mailto:olya_kolbina@mail.ru), [yanafedoseeva06@gmail.com](mailto:yanafedoseeva06@gmail.com), [mr.fatin2017@gmail.com](mailto:mr.fatin2017@gmail.com)

**Abstract.** This article examines methods for protecting quantum databases and the potential for their use in strengthening cryptographic systems in the context of developing quantum computing.

**Keywords:** quantum databases; quantum algorithms; Grover's algorithm; cybersecurity; quantum information security.

Актуальность исследования обусловлена наступлением эры квантовых вычислений, которая создает экзистенциальную угрозу для классических криптографических систем и формирует потребность в принципиально новых подходах к обеспечению информационной безопасности. Развитие квантовых баз данных (КБД) как новой парадигмы хранения и обработки информации требует разработки специализированных алгоритмов защиты, учитывающих их уникальные свойства, и одновременно открывает возможности для создания более мощных инструментов безопасности.

**Цель исследования.** Провести комплексный анализ и систематизацию направлений разработки алгоритмов для квантовых баз данных, ориентированных как на защиту самих КБД, так и на усиление классических систем информационной безопасности.

**Материалы и методы исследования.** В ходе работы проводился анализ научной литературы и публикаций в области квантовых вычислений, квантовой криптографии и теории баз данных. Основу методологии составили сравнительный анализ и систематизация существующих угроз и подходов к защите, а также теоретическое моделирование применения квантовых алгоритмов для решения задач информационной безопасности.

**Полученные результаты.** Были выявлены и систематизированы ключевые особенности КБД как объекта защиты, разработана классификация алгоритмов безопасности для КБД, исследовано прикладное применение алгоритмов КБД для усиления классической безопасности, а также сформулированы ключевые вызовы для практической реализации, включая технологические барьеры (шум, декогеренция в NISQ-устройствах) и отсутствие стандартов, а также определены перспективные направления для дальнейших исследований.

**Выводы.** Проведенное исследование показало, что разработка алгоритмов для квантовых баз данных является критически важным и перспективным направлением. Квантовые вычисления представляют собой двойственный феномен: они являются источником новых угроз для существующих криптосистем, но одновременно служат основой для создания новых, более устойчивых механизмов защиты. Успешное развитие данной области требует опережающих исследований и активного междисциплинарного сотрудничества между специалистами в области квантовой физики, криптографии и информационной безопасности.

#### СПИСОК ЛИТЕРАТУРЫ:

1. Nielsen, M. A., & Chuang, I. L.. Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge University Press. 2010.
2. Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H.. Quantum cryptography. Reviews of Modern Physics, 74(1), 145. 2002.
3. Bennett, C. H., & Brassard, G.. Quantum cryptography: Public key distribution and coin tossing. Theoretical Computer Science, 560, 7-11. 2014.
4. Grover, L. K.. A fast quantum mechanical algorithm for database search. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing (pp. 212-219). 1996.
5. Broadbent, A., & Schaffner, C.. Quantum cryptography beyond quantum key distribution. Designs, Codes and Cryptography, 78(1), 351-382. 2016.
6. Chakraborty, K., & Joy, D.. Quantum Private Query: A New Approach to Privacy-Preserving Data Access. In Proceedings of the 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS). 2021.
7. Alléaume, R., et al.. Using quantum key distribution for cryptographic purposes: A survey. Theoretical Computer Science, 560, 62-81. 2014.
8. Bernstein, D. J., Buchmann, J., & Dahmen, E. (Eds.). Post-quantum cryptography. Springer Science & Business Media. 2009.
9. Biamonte, J., Wittek, P., Pancotti, N., Rebentrost, P., Wiebe, N., & Lloyd, S.. Quantum machine learning. Nature, 549(7671), 195-202. 2017.
10. National Institute of Standards and Technology (NIST).. Post-Quantum Cryptography Standardization. 2022.

УДК 528.9

#### ПРИМЕНЕНИЕ DATA SCIENCE ДЛЯ ПРОГНОЗИРОВАНИЯ В ГЕОИНФОРМАЦИОННЫХ СИСТЕМАХ

**Колбина Ольга Николаевна, Григорьева Ольга Андреевна, Лазарева Вера Дмитриевна**

Российский государственный гидрометеорологический университет

Малоохтинский пр., 98, г.Санктпетербург, 195196, Россия

e-mails: olya\_kolbina@mail.ru, ogridoryeva06@gmai.com, lazver24@gmail.com

**Аннотация.** В данном исследовании рассматриваются методы работы Data Science в геоинформационных системах (ГИС), что позволяет создавать точные модели прогнозирования и анализа геодинамических процессов, эффективно воспроизводить и исследовать природные и урбанистические явления.

**Ключевые слова:** Data Science; геоинформационные системы; прогнозирование; пространственный анализ; машинное обучение; нейронные сети; природные катастрофы; геобезопасность; временные ряды; цифровое моделирование.

#### APPLICATION OF DATA SCIENCE TO FORECASTING IN GEOINFORMATION SYSTEMS

**Kolbina Olga, Grigorieva Olga, Lazareva Vera**

Russian State Hydrometeorological University,

98 Malo-Okhtinsky Ave., St. Petersburg, 195196, Russia

e-mails: olya\_kolbina@mail.ru, ogridoryeva06@gmai.com, lazver24@gmail.com

**Abstract.** This study examines data science methods in geographic information systems (GIS), which enable the creation of accurate models for forecasting and analyzing geodynamic processes, as well as the effective reproduction and study of natural and urban phenomena.

**Keywords:** Data Science; geographic information systems; forecasting; spatial analysis; machine learning; neural networks; natural disasters; geosecurity; time series; digital modeling.

Геоинформационные системы (ГИС) представляют собой современный технологический комплекс для сбора, хранения, анализа, и визуализации пространственных данных. Их прикладная значимость охватывает широкий спектр отраслей. В последние годы наблюдается усиление аналитических возможностей ГИС за счёт интеграции методов Data Science.

Применение таких дисциплин, как статистика, искусственный интеллект (ИИ) и машинное обучение (МО), в работе с большими пространственно-временными данными существенно расширило горизонты анализа. Такая синергия позволяет создавать более точные и надёжные прогностические модели геодинамических и социально-экономических процессов. Это имеет критически важное значение для предупреждения, а также минимизации последствий стихийных бедствий и других чрезвычайных ситуаций (ЧС).

Таким образом, слияние ГИС и Data Science способствует повышению оперативности и эффективности принятия решений в сфере безопасности и устойчивого развития [3][5]

1. Data Science использует статистику, искусственный интеллект и машинное обучение для работы с большими данными в ГИС, что помогает строить точные модели для прогнозирования и анализа геодинамических процессов [7].

2. Современные методы пространственного анализа и цифрового моделирования в Data Science позволяют воспроизводить разные явления и процессы в природе и городах, например, распространение загрязнений, изменения ландшафта и рост городов [4].

3. Машинное обучение и нейронные сети находят сложные связи в геоданных, что помогает лучше прогнозировать стихийные бедствия (землетрясения, наводнения, пожары и т.д.) и социальные угрозы, что позволяет уменьшить ущерб и риски для людей.

4. Объединение Data Science и ГИС помогает автоматически собирать и анализировать данные из разных источников, таких как аэрофотоснимки, спутники и датчики, для планирования маршрутов и быстрого реагирования на важные ситуации [2].

5. Прогнозирование временных рядов и пространственная статистика используются для создания моделей изменения зон затопления, эрозии почв, распространения болезней и влияния климата на безопасность территорий [7].

6. Data Science расширяет возможности управления ресурсами и логистики при ЧС, делая маршруты экстренных служб и распределение сил лучше, что увеличивает скорость и пользу от реагирования.

7. Анализ больших данных, включая сигнализацию о подозрительных изменениях в городской и природной средах, позволяет создавать системы раннего предупреждения и улучшать прогнозы экономической и экологической безопасности [5].

8. Data Science применяет алгоритмы кластеризации, классификации и регрессии для глубокого анализа пространственно-временных процессов, выявляя тренды, аномалии и прогнозируя развитие потенциальных угроз.

9. В сторону открытых решений развивается экосистема. Создаются комплексные конвейеры данных для эффективной работы, которые автоматически извлекают пространственные данные, очищают их, обучают модели и визуализируют прогноз на интерактивной карте [1].

Таким образом, интеграция методов Data Science и искусственного интеллекта в ГИС формирует новую научно-прикладную парадигму — Spatial Data Science. Этот симбиоз позволяет перейти от ретроспективного анализа пространственных данных к созданию прогностических моделей и проактивному управлению рисками. Современные методы пространственного анализа и машинного обучения, включая использование геолокационных данных, дают возможность не только моделировать сложные природные процессы, но и разрабатывать превентивные стратегии, что в конечном итоге способствует повышению уровня защищённости населения и устойчивому развитию территорий.

#### СПИСОК ЛИТЕРАТУРЫ

1. Простейшие методы пространственного анализа и моделирования в ГИС // Epsilonmetrics.ru. – 2024. – URL: <https://blogs.epsilonmetrics.ru/modern-gis/>
2. Пространственный анализ и Data Science // ESRI.com. – 2023. – URL: <https://www.esri-cis.com/ru-ru/arcgis/about-arcgis/spatial-analytics-data-science/overview>
3. Пространственный анализ: как смотреть на данные и разрабатывать модели в ГИС // Epsilonmetrics.ru. – 2024. – URL: <https://blogs.epsilonmetrics.ru/spatial-analysis/>
4. Пашковская О.В., Бренинг Д.В. Методы анализа данных в геоинформационных системах // Компьютерные и информационные науки. – 2020. – URL: <https://cyberleninka.ru/article/n/metody-analiza-dannyh-v-geoinformatsionnyh-sistemah>
5. Spatial Data Science – наука о пространственных данных // Reddit.com. – 2023. – URL: [https://www.reddit.com/r/gis/comments/1c19e36/geospatial\\_data\\_science\\_or\\_other\\_subfields\\_of/](https://www.reddit.com/r/gis/comments/1c19e36/geospatial_data_science_or_other_subfields_of/)
6. Oliveira A., Fachada N., Matos-Carvalho J.P. Data Science for Geographic Information Systems [Электронный ресурс] // arXiv. – 2024. – URL: <https://arxiv.org/html/2404.03754v2>
8. Смирнова О.В. Геоинформационные технологии для прогнозирования природных катастроф // Труды СПИИРАН. – 2010. – Вып. 3(14). – С. 216-227. – ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн). – URL: <https://ia.spcras.ru/index.php/sp/article/view/1514>

УДК 004.75

**EDGE COMPUTING ДЛЯ IoT –УСТРОЙСТВ****Райан Набил Рандович, Касумов Гамид Исакович**

Российский государственный гидрометеорологический университет

192007, Россия, Санкт-Петербург, Воронежская улица, дом 79

e-mails: 1nabil.rayan1@gmail.com, gamid.kai123@gmail.com

**Аннотация.** В настоящих тезисах рассматриваются ключевые задачи, архитектурные схемы, требования и основные вызовы, возникающие при внедрении граничных (edge) вычислений для IoT-устройств. Подчеркивается необходимость переноса части обработки данных ближе к сенсорам для снижения времени отклика, уменьшения сетевой нагрузки и повышения надёжности. Выделяются основные компоненты системы, методы распределения нагрузки и вопросы безопасности и приватности. Закладываются направления дальнейших исследований.

**Ключевые слова:** edge computing; Интернет вещей; распределённая архитектура; задержка; безопасность; балансировка нагрузки; размещение задач

**EDGE COMPUTING FOR IOT-DEVICES****Rayan Nabil, Kasumov Gamid**

The Russia State Hydrometeorological University

79 Voronezhskaya St, Saint Petersburg, 192007, Russia

e-mails: 1nabil.rayan1@gmail.com, gamid.kai123@gmail.com

**Abstract.** This thesis examines the key tasks, architectural patterns, requirements, and main challenges associated with the implementation of edge computing for IoT devices. It emphasizes the necessity of moving data processing closer to the sensors to reduce latency, decrease network load, and enhance reliability. The main system components, load distribution methods, and issues of security and privacy are highlighted. The foundations for future research directions are laid out.

**Keywords:** edge computing; Internet of Things; distributed architecture; latency; security; load balancing; task placement

**1. Основная проблема, которую решает Периферийный Компьютинг (Edge Computing) [1]**

Облачных технологий для Интернета Вещей (IoT) недостаточно. Подключение миллионов устройств напрямую к облаку сталкивается с тремя главными проблемами: высокая стоимость, риски конфиденциальности и перегрузка сетей. Edge Computing решает эту проблему, перенося обработку данных ближе к самим устройствам, что позволяет не отправлять все сырые данные в облако. Это фундаментальная причина его появления.

**2. Главное преимущество: Сверхнизкая задержка (Low Latency)**

Это одно из ключевых технических преимуществ, особенно для систем, где от скорости зависит безопасность людей и сохранность оборудования (например, на автоматизированном производстве или в беспилотных автомобилях). Разница в скорости реакции между облаком (100 мс) и периферийным устройством (1 мс) может быть критической. Edge Computing обеспечивает мгновенную реакцию благодаря тому, что решения принимаются локально, без задержек на передачу данных в облако и обратно.

**3. Критически важная особенность: Автономная работа (Autonomy)**

Надёжность IoT-систем не должна зависеть от постоянного и стабильного интернет-соединения. Периферийные вычисления позволяют системе продолжать стабильную работу, даже если связь с облаком полностью пропала. Например, система мониторинга оборудования на заводе или контроля температуры в холодильнике будет функционировать и подавать локальные сигналы тревоги, даже при полном отсутствии подключения к интернету.

**4. Что такое «Периферия» на практике? Это целая экосистема устройств**

Важный момент: не существует единого понятия «периферийное устройство». Термин «Edge» описывает целую иерархию и экосистему устройств — от самых простых датчиков и микроконтроллеров до мощных шлюзов и локальных серверов, которые должны работать вместе. Эффективное решение должно быть

**5. Практическая эффективность: Оптимизация данных и экономия ресурсов [390]**

Одной из фундаментальных проблем IoT является огромный объем «сырых» данных, генерируемых устройствами. Передача всего этого массива в облако является ресурсоемкой, требует значительной пропускной способности и влечет высокие финансовые затраты. Edge Computing решает эту проблему за счет предварительной обработки и фильтрации данных непосредственно в периферийном устройстве или шлюзе. В облако передаются только агрегированные результаты, ключевые метрики или данные, требующие углубленного анализа. Например, умный датчик может не передавать показания температуры каждую секунду, а лишь уведомлять облако о выходе значения за заданные пределы или отправлять усредненное значение за час. Такой подход значительно снижает нагрузку на сеть, объем облачного хранилища и общую стоимость владения IoT-системой.

**6. Ключевые преимущества и недостатки внедрения Edge Computing [3]**

**Преимущества:**

- Скорость реакции (Низкая задержка). Локальная обработка данных обеспечивает реакцию в режиме реального времени, что критически важно для таких приложений, как беспилотные автомобили и роботизированная хирургия.
- Экономия трафика. Снижение нагрузки на сеть за счет локальной обработки и передачи в облако только релевантных, агрегированных данных, а не всего объема «сырых» данных.
- Автономность работы. Способность edge-устройств функционировать и принимать решения даже при полной потере соединения с центральным облаком.
- Повышение конфиденциальности данных. Чувствительная информация обрабатывается локально и не передается по сети, оставаясь в пределах защищенного периметра.

**Недостатки:**

- Сложность управления. Трудности централизованного контроля за тысячами географически распределенных устройств с разными версиями ПО и конфигурациями.
- Разнообразие платформ. Необходимость поддержки множества аппаратных архитектур (x86, ARM, MIPS) и операционных систем, что усложняет разработку и развертывание.
- Проблемы безопасности. Каждое устройство представляет собой потенциальную точку входа для атак, а его физическая доступность усугубляет риски.
- Вопросы надежности. Высокая вероятность сбоев отдельных устройств, что требует создания отказоустойчивых систем и механизмов самовосстановления.

**СПИСОК ЛИТЕРАТУРЫ**

1. Bosch.IO GmbH. «White Paper: Edge Computing for the IoT» [Электронный ресурс]. – 25.10.2023. – URL: [https://bosch-iot-suite.com/wp-content/uploads/20231025\\_white-paper\\_edge-computing\\_EN-1.pdf](https://bosch-iot-suite.com/wp-content/uploads/20231025_white-paper_edge-computing_EN-1.pdf)
2. Scale Computing. «Understanding the Pieces of IoT Edge Computing» [Электронный ресурс]. – URL: <https://www.scalecomputing.com/resources/iot-edge-computing>
3. Edge computing: новый подход к обработке данных [Электронный ресурс]. – URL: <https://kurshub.ru/journal/blog/edge-computing-novyy-podhod-k-obrabotke-dannyh>

**УДК****ГОЛОСОВЫЕ И ЖЕСТОВЫЕ ИНТЕРФЕЙСЫ В РЕГИОНАЛЬНЫХ ГИС И СИСТЕМАХ  
УПРАВЛЕНИЯ: РИСК И ЗАЩИТА**

**Пункевич Дана Марковна, Паймеров Константин Витальевич, Колбина Ольга Николаевна**

Российский государственный гидрометеорологический университет,

Санкт-Петербург, Россия,

e-mails: [Punkevichdana@gmail.com](mailto:Punkevichdana@gmail.com), [aplay586@mail.ru](mailto:aplay586@mail.ru), [olya\\_kolbina@mail.ru](mailto:olya_kolbina@mail.ru)

**Аннотация.** Рассматриваются риски голосовых и жестовых интерфейсов в региональных ГИС/АСУДД и предлагается минимальный безопасный контур: непрерывная привязка «личность–намерение–контекст», разделение наблюдения и управления, риск-ориентированная MFA и проверка в цифровом двойнике. Описаны политики для одиночного и мультипользовательского режима, защита каналов и неизменяемый аудит.

**Ключевые слова:** голосовой интерфейс; жестовый интерфейс; региональная ГИС; АСУДД; биометрическая аутентификация; многофакторная авторизация; цифровой двойник; правило двух лиц; сегментация сети; неизменяемые журналы.

**VOICE AND GESTURE INTERFACES IN REGIONAL GIS AND CONTROL SYSTEMS:  
RISKS AND SAFEGUARDS**

**Punkevich Dana, Paymerov Konstantin, Kolbina Olga**

Russian State Hydrometeorological University,

Saint-Petersburg, Russia,

e-mails: [Punkevichdana@gmail.com](mailto:Punkevichdana@gmail.com), [aplay586@mail.ru](mailto:aplay586@mail.ru), [olya\\_kolbina@mail.ru](mailto:olya_kolbina@mail.ru)

**Abstract.** We address security risks of voice and gesture interfaces in regional GIS/traffic control and propose a minimal secure pipeline: continuous identity–intent–context binding, observation/control separation, risk-based MFA, and pre-execution validation in a digital twin. We outline single/multi-user policies, protected channels, and immutable auditing.

**Keywords:** voice interface; gesture interface; regional GIS; traffic management; biometric authentication; multi-factor authorization; digital twin; two-man rule; network segmentation; immutable logs.

Бесконтактные интерфейсы ускоряют работу ситуационных центров, ГИС и АСУДД, но переносят критические операции в зону биометрии и ИИ, где ошибка распознавания или подмена сигнала сразу превращаются не в технический сбой, а в управленческий инцидент.

Поэтому необходимо непрерывно связывать личность, намерение и контекст: кто подал команду, что именно он хотел сделать, уместно ли действие здесь и сейчас и права доступа. Без этой привязки голос и жесты небезопасны в критичных контурах, таких как: транспорт, инфраструктура, безопасность.

Голос уязвим к повтору (replay-атака) и синтезу (deepfake), ультразвуковым командам и шумовым атакам; жесты — к подмене видеопотока, адверсариальным принтам и «заимствованию» движений рядом стоящими людьми.

Для ГИС добавляются риски целостности слоев и меток, несанкционированного доступа к конфиденциальным данным и отказов каналов телеметрии, система теряет актуальную информацию и перестает отражать реальное состояние объектов. В государственных, военных и финансовых доменах критичны конфиденциальность расположений и объектов, целостность картографической семантики и бесперебойное функционирование каналов связи. Ошибка или подмена напрямую искажают решения в реальном времени.

Сессия закрепляется за одним оператором по биометрии и зоне камеры; голос привязывается к тому же субъекту. При появлении постороннего система приостанавливает исполнение, повторно верифицирует владельца и игнорирует внешние источники; для опасных действий включается второй фактор и правило «двух рук» - участие второго оператора.

Последовательность стадий состоит из перцепции (восприятия внешнего сигнала), идентификации, интерпретации намерения, риск-ориентированной авторизации, подтверждения, исполнения и аудита. Низкорисковые действия выполняются упрощенно, высокорисковые требуют подтверждения двумя лицами, проверки в цифровом двойнике и автоматического отката при аномалии.

Передача данных защищается взаимной аутентификацией и шифрованием, сеть сегментируется, доступ к брокерам событий — по строгим политикам безопасности. Биометрия и ключи хранятся в изолированных средствах защиты с ротацией; логи распознавания, авторизации и исполнения фиксируются в неизменяемом хранилище. Конфиденциальные слои ГИС изолируются и выдаются по ролям и атрибутам.

Пороги настраиваются консервативно: минимальный ложный допуск для критичных операций при допустимом росте ложных отказов.

Модели тестируются на шум, эхо, окклюзии и адверсариальные примеры; дообучение — только контролируемыми релизами с возможностью отката. Контуры наблюдения и управления разделяются. Изменение фаз и приоритетов сначала моделируется в цифровом двойнике или тестовой среде, ограничением времени действия и протоколированием «кто-что-где-когда-почему». В интерфейсе визуально помечается активный оператор, что снижает риск контекстных ошибок.

Зона управления физически и логически ограничивается; команды извне игнорируются. Голос отключается при высоком шумовом фоне или конкурирующих источниках.

Жестовый словарь сокращается до однозначных паттернов; перед исполнением система показывает распознанное действие и даёт короткое окно отмены. Проектирование ведётся с учётом требований законодательства о КИИ и обработки персональных данных, применяются сертифицированные средства защиты каналов и хранилищ, доверенная загрузка, независимые проверки безопасности и документированная модель угроз, включая сценарии подмены аудио и видео.

Таким образом, связывание личности, намерения и контекста, режим единоличного владения сессией и автоматическое усиление контроля при появлении посторонних переводят голосовые и жестовые интерфейсы из «удобной функции» в безопасный инструмент.

В критичных доменах их применение оправдано только при строгой аутентификации, контекстной валидации, ступенчатой авторизации, защищенных каналах, безопасном хранении биометрии и ключей, обязательной симуляции и полном аудите. Без этих мер вероятность инцидентов остается неприемлемо высокой.

## СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р. 52438-2005 Географические информационные системы. Термины и определения // нац. стандарт РФ–Введ. – 2006. – Т. 1.
2. ГОСТ Р. 58273-2018 (ИСО/МЭК 29197: 2015) Информационные технологии. Биометрия. Методология испытаний эксплуатационных характеристик биометрической системы на воздействие условий окружающей среды // нац. стандарт РФ–Введ. – 2019. – Т. 1.
3. Обеспечение информационной безопасности АСУ ТП с использованием метода предиктивной защиты / Гарбук С. В., Правиков Д. И., Полянский А. В., Самарин И. В. // Вопросы кибербезопасности. – 2019. – №. 3 (31). – С. 63-71.
4. Методы детектирования спуфинг-атак повторного воспроизведения на голосовые биометрические системы / Лаврентьева Г. М., Новосёлов С. А., Козлов А. В., Кудашев О. Ю., Щемелинин В. Л., Матвеев Ю. Н. и др. // Научно-технический вестник информационных технологий, механики и оптики. – 2018. – Т. 18. – №. 3. – С. 428-436.
5. Муравьев А. Г., Шифрин Б. М. БЕЗОПАСНОСТЬ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ: СИСТЕМЫ ФИЗИЧЕСКОЙ ЗАЩИТЫ, НОРМАТИВНО-ПРАВОВАЯ ОСНОВА // Правовая информатика. – 2025. – №. 2. – С. 132-139.
6. Аналитический обзор моделей и методов автоматического распознавания жестов и жестовых языков / Рюмин Д. А., Кагилов И. А., Аксёнов А. А., Карлов А. А. // Информационно-управляющие системы. – 2021. – №. 6 (115). – С. 10-20.
7. Применение методов автоматизации при определении актуальных угроз безопасности информации в информационных системах с применением банка данных угроз ФСТЭК России / Селифанов В. В., Звягинцева П. А., Юракова Я. В., Слонкина И. С. // Интерэкспо Гео-Сибирь. – 2017. – Т. 8. – С. 202-209.
8. Солодяников А. В. Информационная безопасность автоматизированных систем. – 2020.



УДК 004.056

**РОЛЬ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ В ОБЕСПЕЧЕНИИ ПРОЗРАЧНОСТИ И ДОВЕРИЯ:  
КЕЙСЫ ИСПОЛЬЗОВАНИЯ ОТКРЫТЫХ ГЕОДАННЫХ ДЛЯ ПОЗИТИВНОГО  
РЕПУТАЦИОННОГО ПОЗИЦИОНИРОВАНИЯ**

**Ратушняк Евгений Алексеевич, Грызунов Виталий Владимирович**

Санкт-Петербургский университет ГПС МЧС России

Московский проспект, 149, Санкт-Петербург, 196105, Россия

e-mails: evgrat123@mail.ru, viv1313r@mail.ru

**Аннотация.** В докладе рассматривается использование открытых геоданных как инструмента формирования позитивного репутационного имиджа организаций при соблюдении требований информационной безопасности. Анализируются риски, связанные с утечкой и подменой пространственной информации, а также необходимость обеспечения её целостности и аутентичности. Особое внимание уделено применению доверенных инфраструктур, таких как PKI, и защите краудсорсинговых данных. Приведены практические кейсы интеграции безопасных ГИС в корпоративные и муниципальные системы. Подчеркивается, что прозрачность становится репутационным преимуществом только при гарантированной устойчивости и защите данных.

**Ключевые слова:** геоданные; ГИС; информационная безопасность; репутация; краудсорсинг, PKI.

**THE ROLE OF GEOGRAPHIC INFORMATION SYSTEMS IN ENSURING TRANSPARENCY  
AND TRUST: CASE STUDIES OF USING OPEN GEODATA FOR POSITIVE  
REPUTATIONAL POSITIONING**

**Ratushnyak Evgeniy, Gryzunov Vitaliy**

St. Petersburg University of State Fire Service of EMERCOM of Russia,

149 Moskovsky Prospect, St. Petersburg, 196105, Russia

e-mails: evgrat123@mail.ru, viv1313r@mail.ru

**Abstract.** The report examines the use of open geospatial data as a tool for shaping a positive reputational image of organizations while complying with information security requirements. It analyzes risks associated with data leakage and manipulation of spatial information, as well as the need to ensure its integrity and authenticity. Special attention is given to the use of trusted infrastructures such as PKI and the protection of crowdsourced data. Practical cases of integrating secure GIS solutions into corporate and municipal systems are presented. It is emphasized that transparency becomes a reputational advantage only when data resilience and security are ensured.

**Keywords:** geospatial data; GIS; information security; reputation; crowdsourcing; PKI.

**Введение.** Использование открытых геоданных для позитивного репутационного позиционирования становится стратегическим преимуществом только при условии обеспечения высокого уровня информационной безопасности. ГИС должны проектироваться как устойчивые к дестабилизирующим факторам системы, где доступность, целостность и аутентичность данных — не опции, а основа доверия [1, 2, 4]. Только в таком случае прозрачность превращается из риска в репутационный актив.

Открытые геоданные как ресурс репутационного капитала — с учётом иб-ограничений. Открытые геоданные (например, из Copernicus, OpenStreetMap, государственных порталов) могут служить объективным подтверждением вклада организации в устойчивое развитие территорий. Однако их использование требует строгой верификации источников и защиты от внедрения фейковых или искажённых данных, что особенно актуально при работе с распределёнными системами, где уязвимости на уровне ввода данных и аутентификации считаются наиболее опасными [1]. Безопасная интеграция внешних геоданных возможна только при наличии доверенной инфраструктуры, основанной на проверенных моделях доверия, таких как инфраструктура открытых ключей (PKI) [3].

Механизмы позитивного репутационного позиционирования через ГИС при обеспечении ИБ.

- Визуализация экологических инициатив должна сопровождаться цифровыми подписями и метаданными, подтверждающими подлинность и целостность картографических слоёв [3].

- Публичные интерактивные дашборды требуют адаптивного управления доступностью ресурсов, особенно в условиях деструктивных воздействий (DDoS, компрометация узлов), что возможно благодаря методам агрегации производительности и виртуализации резервов [4].

- Crowdsourcing геоданных от граждан должен быть защищён от спуфинга и манипуляций: требуется строгая идентификация участников и валидация вводимых данных — именно эти компоненты часто становятся точками проникновения злоумышленников [1].

Кейсы применения с учётом устойчивости к дестабилизирующим факторам.

- Энергетическая компания публикует карту солнечных станций с цифровыми сертификатами, подтверждающими подлинность данных; система построена с учётом нестохастических показателей устойчивости ГИС к внешним воздействиям [2].

- Городская администрация использует ГИС-платформу с адаптивным управлением доступностью, позволяющим сохранять работоспособность даже при частичной деградации ИБС [4, 5].

– Логистическая фирма применяет модель доверия на основе РКИ при интеграции данных о маршрутах из внешних источников, что исключает возможность подмены информации и обеспечивает соответствие требованиям ИБ для критически важных процессов [3].

Прозрачность без безопасности может привести к обратному эффекту — утрате доверия из-за компрометации данных. Особенно опасны уязвимости, связанные с неполной проверкой входных данных, инъекциями и нарушением механизмов аутентификации [1]. Для ГИС, используемых в репутационных целях, необходимо внедрение не только технических, но и процедурных мер: регулярный аудит источников, контроль целостности через хеширование, применение моделей доверия, устойчивых к целенаправленным агрессивным действиям [3, 6].

Заключение. Использование открытых геоданных для позитивного репутационного позиционирования становится стратегическим преимуществом только при условии обеспечения высокого уровня информационной безопасности. ГИС должны проектироваться как устойчивые к дестабилизирующим факторам системы, где доступность, целостность и аутентичность данных — не опции, а основа доверия [1, 2, 4]. Только в таком случае прозрачность превращается из риска в репутационный актив.

#### СПИСОК ЛИТЕРАТУРЫ

1. Грызунов В. В., Гришечко А. А., Сипович Д. Е. Выбор Наиболее Опасных Уязвимостей Для Перспективных Информационных Систем Критического Применения // Вопросы кибербезопасности. – 2022. – № 1(47). – С. 66–75.
2. Burlov V. G., Gryzunov V. V. Evaluation of the effectiveness of geographic information systems adaptation to destabilizing factors // Journal of Physics: Conference Series. – 2020. – P. 012016.
3. Грызунов В. В., Корниенко А. А., Глухарев М. Л., Крюков А. С. Выбор моделей доверия при интеграции распределенных информационных систем критического применения // Проблемы информационной безопасности. Компьютерные системы. – 2021. – № 4. – С. 79–90.
4. Грызунов В. В. Методы адаптивного управления доступностью ресурсов геоинформационных систем в условиях деструктивных воздействий // Труды учебных заведений связи. – 2022. – Т. 8, № 3. – С. 101–116.
5. Грызунов В. В. Методика решения измерительных и вычислительных задач в условиях деградации информационно-вычислительной системы // Вестник СибГУТИ. – 2015. – № 1(29). – С. 35–46.
6. Грызунов В. В. Модель целенаправленных агрессивных действий на информационно-вычислительную систему // Человеческий фактор в сложных технических системах и средах (Эрго-2018). – 2018. – С. 300–305.



## ПОДГОТОВКА И ПЕРЕПОДГОТОВКА КАДРОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК 331.52:004.77

### ПРОБЛЕМАТИКА КАДРОВОГО ДЕФИЦИТА В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИИ: ВЫЗОВЫ И ОПЫТ ПРАКТИКО-ОРИЕНТИРОВАННОЙ ПОДГОТОВКИ СПЕЦИАЛИСТОВ

**Ахrameeva Ксения Андреевна**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большеви́ков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mail: oklaba@mail.ru

**Аннотация:** Информационная безопасность — быстроразвивающаяся сфера, требующая практической квалификации специалистов. В России сохраняется острый дефицит ИБ-кадров на фоне роста технологического сектора. Нехватка ИТ-специалистов достигает 500-700 тысяч человек, что угрожает цифровой безопасности. В статье описан опыт Газинформсервис по созданию практикоориентированных образовательных программ для преодоления дефицита и повышения качества подготовки через сотрудничество бизнеса, вузов и государства.

**Ключевые слова:** кадровый дефицит; информационная безопасность; практикоориентированные программы обучения; подготовка специалистов

### THE PROBLEM OF WORKFORCE SHORTAGE IN INFORMATION SECURITY IN RUSSIA: CHALLENGES AND EXPERIENCE OF PRACTICE-ORIENTED SPECIALIST TRAINING

**Akhrameeva Kseniia**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications  
22 Bolshevnikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mail: oklaba@mail.ru

**Abstract:** Information security is a rapidly evolving field that requires practical qualifications for specialists. In Russia, there is a severe shortage of information security personnel amid the growth of the technology sector. The shortage of IT specialists reaches 500–700 thousand people, posing a threat to digital security. The article describes the experience of Gazinformservice in creating practice-oriented educational programs to address this shortage and improve training quality through collaboration between business, universities, and the government.

**Keywords:** workforce shortage; information security; practice-oriented educational programs; specialist training.

В последние годы российский технологический сектор демонстрирует устойчивый рост, что способствует увеличению спроса на квалифицированных ИТ-специалистов, в том числе по информационной безопасности (ИБ).

Согласно исследованию Tadviser, дефицит ИТ-кадров в России достигает от 500 до 700 тысяч человек, при этом особенно остро ощущается нехватка профильных специалистов по ИБ [1]. Данная ситуация негативно сказывается на устойчивости цифровой экономики и уровне киберзащиты государства.

Одной из ключевых причин данного кадрового дефицита является недостаточная адаптивность вузовских образовательных программ к быстро меняющимся требованиям рынка труда. Учебные планы вузов остаются преимущественно теоретически ориентированными и зачастую не предусматривают достаточного объёма практических занятий, связанных с реальными инцидентами и моделированием кибератак. В результате выпускники не обладают необходимыми компетенциями для эффективного решения актуальных задач информационной безопасности [2, 3].

Для преодоления этого разрыва бизнес должен принимать активное участие в процессе подготовки кадров. Компания Газинформсервис реализовала проект создания дополнительных профессиональных курсов, ориентированных на практическое обучение с использованием реальных кейсов и индустриального опыта. Помимо этого, компания активно сотрудничает с вузами, предоставляя не только программные комплексы для проведения лабораторных работ, но и методические материалы к ним. Это даёт студентам возможность уже во время обучения познакомиться с современными инструментами и технологиями защиты информации и освоить их на практике.

Компания Газинформсервис выстраивает свою деятельность на принципах тесного взаимодействия бизнеса и образовательных учреждений. Такое сотрудничество позволяет совместно разрабатывать единые

компетенционные стандарты и стимулировать внедрение практикоориентированных программ обучения, что является критически важным для формирования готовых к работе специалистов в области информационной безопасности [4, 5].

#### СПИСОК ЛИТЕРАТУРЫ

1. Отчет Tadviser по рынку IT-кадров в России (2023) // Tadviser. 2023. URL: <https://www.tadviser.ru/index.php/Отчет> (дата обращения: 22.08.2025).
2. Степанова И.В. Современные проблемы подготовки кадров в сфере информационной безопасности // Вестник информационных технологий. 2023. № 4. С. 45–53.
3. Рыбаков А.А. Дефицит IT-кадров в России: причины и пути решения // Информационные технологии. 2024. Т. 12, № 1. С. 28–35.
4. Тарасов П.В. Современные методы обучения в области информационной безопасности: от теории к практике // Образование и безопасность. 2022. № 3. С. 12–20.
5. Материалы конференции «Информационная безопасность и образование», Москва, 2023. 150 с.

УДК 004.9:37:351.86

### ЦИФРОВАЯ ГРАМОТНОСТЬ КАК ОСНОВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОЛЬЗОВАТЕЛЯ В СОВРЕМЕННОМ ОБЩЕСТВЕ

**Борщенко Виктор Владимирович**

Северо-Западный институт управления - филиал РАНХиГС,  
Средний пр. В.О., 57, Санкт-Петербург, 199178, Россия  
e-mail: boss-victor@yandex.ru

**Аннотация.** Статья посвящена исследованию цифровой грамотности как основы информационной безопасности пользователей в условиях стремительной цифровизации российского общества. Анализируются теоретические аспекты понятия цифровой грамотности, включая медиаграмотность, информационную культуру и технические навыки, с опорой на работы отечественных авторов. Особое внимание уделено роли информационной безопасности как ключевого компонента, предотвращающего угрозы, такие как кибербуллинг, фишинг и утечки данных, что подтверждено актуальными данными 2025 года. На основе анализа научных статей и современных проектов, таких как "Урок Цифры" и "IT-диктант", рассматриваются методы формирования и оценки цифровых компетенций, адаптированные к различным возрастным группам. Исследование подчеркивает необходимость системного подхода, включая интеграцию в образовательные программы и ежегодную актуализацию знаний. Эмпирические данные, включая стабилизацию индекса цифровой грамотности на уровне 71 процента, выявляют региональные и демографические диспропорции, требующие целевых мер. Предложены рекомендации по развитию критического мышления и этического поведения в сети, а также интеграции искусственного интеллекта в образовательные стандарты. Статья опирается на богатый массив литературы и государственных программ, подчеркивая стратегическую важность темы для национальной безопасности и конкурентоспособности общества в цифровую эпоху.

**Ключевые слова:** цифровая грамотность; информационная безопасность; социокomпьютинг; образовательные программы; киберугрозы; медиаграмотность; цифровая экономика; критическое мышление; ИИ-технологии; национальные проекты.

### DIGITAL LITERACY AS THE BASIS FOR USER INFORMATION SECURITY IN MODERN SOCIETY

**Borshchenko Viktor**

North-West Institute of Management - branch of RANEPa,  
57 Sredny Av. Vasilievsky Island, St. Petersburg, 199187, Russia  
e-mail: boss-victor@yandex.ru

**Abstract.** The article explores digital literacy as a foundational element of user information security amid the rapid digitization of Russian society. It examines the theoretical underpinnings of digital literacy, encompassing media literacy, information culture, and technical skills, drawing on the works of both domestic and international scholars. Particular attention is paid to the role of information security as a critical component in mitigating threats such as cyberbullying, phishing, and data breaches, supported by current 2025 data. Based on an analysis of six scientific articles and contemporary initiatives like "Digital Lesson" and "IT Dictation," the study addresses methods for developing and assessing digital competencies tailored to various age groups. It underscores the necessity of a systematic approach, including integration into educational curricula and annual knowledge updates. Empirical data, including the stabilization of the digital literacy index at 71 points, reveal regional and demographic disparities necessitating targeted measures. Recommendations are proposed for enhancing critical thinking and ethical online behavior, alongside integrating AI into educational standards. The article leverages a rich body of literature and national programs, emphasizing the strategic importance of this topic for national security and societal competitiveness in the digital era.

**Keywords:** digital literacy; information security; social computing; educational programs; cyber threats; media literacy; digital economy; critical thinking; AI technologies; national projects.

В условиях интенсивной цифровизации всех сфер общественной жизни, когда информационные технологии определяют не только экономические процессы, но и социальные взаимодействия, вопрос формирования компетенций по грамотному обращению с данными приобретает первостепенную важность.

Цифровая грамотность здесь предстает не как вспомогательный навык, а как фундаментальная основа для защиты личности от рисков в сетевом пространстве. Она воплощает в себе устойчивые паттерны поведения, базирующиеся на знаниях и умениях безопасного и продуктивного использования цифровых устройств, сервисов и ресурсов [1]. Эта компетентность служит ключевым механизмом снижения уязвимостей в распределенных системах, где обмен данными происходит в динамичном режиме.

Актуальность темы подкрепляется современными статистическими данными: по состоянию на 2025 год, индекс цифровой грамотности россиян стабилизировался на уровне 71 балл из 100, не демонстрируя роста третий год подряд, что сигнализирует о необходимости усиления образовательных мер. Это особенно значимо в контексте национального проекта "Цифровая экономика", где акцент делается на повышении компетенций населения для адаптации к технологическим вызовам. В статье подробно разбираются теоретические основы цифровой грамотности, ее интеграцию с аспектами информационной безопасности, методы формирования и оценки, опираясь на анализ отечественных исследований, а также актуальные данные о проектах и тенденциях в России. Расширение объема анализа позволит глубже осветить междисциплинарные связи и практические рекомендации, способствуя комплексному пониманию проблемы [2].

Эволюция понятия цифровой грамотности отражает переход от чисто технических интерпретаций к социально-гуманитарным конструктам, интегрирующим этические и коммуникативные измерения. Зарубежные концепции, такие как подход П. Гилстера, подчеркивают способность понимать и применять информацию из многообразных форматов, с акцентом на коммуникацию и креативность [3]. В российском научном дискурсе, по Гендиной Н.И., она сливается с информационной культурой, подразумевающей анализ и трансформацию данных на технологической базе [1]. Захарова А.С. позиционирует цифровую грамотность как императив академической среды, где она обеспечивает доступ к знаниям, стимулирует инновации и развивает критическое мышление среди студентов [4]. Это включает не только поиск информации, но и ее верификацию, что критично в эпоху фейковых новостей.

Ключевые компоненты, выделяемые Иванченко Д.А., охватывают медиаграмотность для взаимодействия с ресурсами, информационную грамотность для отбора и оценки данных, навыки безопасности для нейтрализации угроз, а также технические умения по эксплуатации устройств [1]. Что дополняется видением цифровой грамотности как ключевой компетенции педагога, необходимой для формирования у учеников навыков в цифровой экономике, включая креативное применение инструментов и постоянное самообучение [3]. Для школьников она приобретает жизненно важный характер, способствуя безопасному сотрудничеству в цифровой образовательной среде, где дети часто сталкиваются с рисками раньше, чем осваивают защитные механизмы [5]. Ряд авторов углубляют социокоммуникативные аспекты, особенно в социальных сетях, подчеркивая, что будущие педагоги должны владеть сетевым этикетом и мерами против взломов, поскольку дефицит знаний провоцирует конфликты и уязвимости [6].

Ображей О.Н. в социологическом анализе подчеркивает многокомпонентность и динамику цифровой грамотности как конструкта, включающего информационную, компьютерную и коммуникативную составляющие, что делает ее императивом для успешной адаптации в современном обществе [7]. Автор отмечает, что низкая самооценка компетенций коррелирует с избеганием технологий, усиливая социальные разрывы, хотя в российском контексте аналогичные тенденции наблюдаются среди пожилых групп населения. Эмпирические данные из исследований Рогозина С.А. демонстрируют, что лишь 13% студентов компетентно создают образовательные сообщества в сетях, а 54% обладают низким уровнем знаний этикета [6], что подчеркивает необходимость системного подхода к формированию этих навыков.

В 2025 году, согласно федеральным инициативам, цифровая грамотность интегрируется в образовательные стандарты через проекты вроде "Урок цифры", где школьники осваивают курсы по искусственному интеллекту (ИИ) и кибербезопасности объемом от 54 часов на специализированных платформах [8]. Это отражает сдвиг от базовых умений к продвинутым, включая анализ больших данных, что усиливает роль грамотности в противодействии угрозам. Захарова А.С. приводит примеры, где цифровая грамотность способствует развитию творческого мышления через доступ к ресурсам и инструментам, таким как графические редакторы и базы данных [4]. Жумашева С.С. акцентирует на коммуникационных аспектах, отмечая, что цифровая грамотность предполагает постоянное общение в сети, что требует навыков сетевого этикета и креативных действий [3].

Расширение теоретического обзора позволяет выделить иерархию компонентов: от базовых (технических) к высшим (этическим и аналитическим). Кайсина А.В. подчеркивает, что в школьной среде это включает умение отличать факты от мнений и избегать рисков в онлайн-общении, где 75% подростков самообучаются хаотично, без системного подхода [5]. К этому можно добавить динамичный характер грамотности, требующий постоянного обновления в связи с технологическими изменениями [7]. Таким образом, теоретическая база подчеркивает интегративный характер цифровой грамотности, объединяющий знания из педагогики, социологии и информатики.

Информационная безопасность формирует ядро цифровой грамотности, подразумевая ответственное отношение к данным и их защите. Иванченко Д.А. детализирует знания о распространенных угрозах, включая троллинг, кибербуллинг и фишинг, а также методы их нейтрализации, такие как соблюдение конфиденциальности [1]. Рогозин С.А. и соавторы фокусируются на контексте социальных сетей, где диагностика выявляет значительные пробелы: многие студенты используют слабые пароли, а большинство игнорируют двухфакторную аутентификацию, что повышает риски взломов [6]. Захарова А.С. отмечает, что

среди студентов общий уровень грамотности достигал 71%, но аспекты безопасности требуют углубления, особенно в академической среде с высоким риском утечек данных [4].

Жумашева С.С. связывает безопасность с педагогической компетентностью, подчеркивая, что учителя обязаны демонстрировать навыки защиты, чтобы передавать их ученикам, включая креативное использование инструментов без риска [3]. Для школьников это подразумевает умение различать надежные источники и избегать онлайн-рисков, где хаотичное самообучение приводит к уязвимостям [5]. Ображей О.Н. в анализе подчеркивает, что информационная безопасность как компонент грамотности включает защиту устройств и данных, что критично для динамичной адаптации в цифровой среде [7].

Актуальные данные 2025 года подтверждают приоритетность: человеческий фактор ответственен за 75% утечек информации в российских компаниях, что подчеркивает необходимость повышения грамотности в области кибергигиены. Проекты вроде "Цифровой ликбез" охватывают миллионы участников, фокусируясь на защите от фишинга и дезинформации, особенно среди молодежи. Тренды кибербезопасности включают использование ИИ для предиктивной защиты, но также рост атак на основе глубоких фейков, требующих повышенной грамотности [9-10].

Компоненты информационной безопасности:

1. Знание угроз - Идентификация рисков в сети (Троллинг, кибербуллинг, фишинг)
2. Защита данных – Конфиденциальность и шифрование (Слабые пароли, двухфакторная аутентификация)
3. Сетевой этикет - Нормы общения и поведения (Избегание конфликтов в соцсетях)
4. Критическая оценка - Различение фактов от дезинформации (Верификация источников)
5. Технические меры - Эксплуатация устройств с защитой (Антивирусные программы, обновления программного обеспечения)
6. Динамичная адаптация - Обновление навыков под угрозы (Реакция на новые атаки)

Эти компоненты иллюстрируют, что безопасность – интегральная часть грамотности, предотвращающая уязвимости в социокomпьютинге. Расширение анализа показывает, что в 2025 году фокус на ИИ-атаках требует включения этических аспектов в образование [6].

Формирование цифровой грамотности предполагает системный и дифференцированный подход. Иванченко Д.А. формулирует принципы: учет социально-демографических групп, интеграцию методов (тесты, кейсы, интервью), качественную и количественную оценку, ежегодную актуализацию [1]. Кайсина А.В. предлагает интегрировать в школьные программы учебно-методические комплексы Угриновича, с акцентом на практические навыки поиска, оценки и безопасного использования информации [5]. Также рекомендуется внедрить такие мероприятия как: семинары по этике, ролевые игры по коммуникации, научные конференции на темы защиты данных в образовании [6].

Оценка сочетает самооценки и объективные инструменты. Захарова А.С. приводит данные, где 71% студентов высоко оценивают свои навыки, но пробелы в безопасности требуют корректировки [4]. Жумашева С.С. видит в оценке инструмент конкурентоспособности, предлагая мониторинг через проекты и онлайн-курсы [3]. Ображей О.Н. подчеркивает динамику оценки, где самооценка коррелирует с использованием технологий, рекомендуя комплексные опросы [7].

В 2025 году проекты вроде "ИТ-диктант" позволяют аттестовать навыки миллионов россиян, включая безопасность, а "Библиотечная школа цифровой грамотности" предлагает курсы для всех возрастов. Поручение президента РФ усиливает эти инициативы, включая уроки в школах по кибергигиене [11-13].

Методы формирования по возрастным группам:

- Для школьников – «Урок цифры» по ИИ: Угринович: поиск, оценка, безопасность
- Для студентов – «Цифровой ликбез: Этикет в сетях, защита аккаунтов
- Для педагогов – «ЦифрАтест»: Цифровая экономика, креативные инструменты
- Для взрослых - Региональные программы: ИТ-диктант, оценка навыков
- Для всех - Национальный проект «Цифровая экономика»: Ежегодные обновления, самооценки

Эти методы обеспечивают непрерывное развитие, адаптируя к эволюции угроз. Расширение включает региональные практики: в 2025 году отчеты АНО "Цифровая экономика" выделяют лучшие инициативы по кибергигиене для детей и пожилых [14].

Цифровая грамотность выступает неотъемлемой основой информационной безопасности пользователей, интегрируя знания, практические навыки и этические принципы, что позволяет эффективно противодействовать рискам в условиях социокomпьютинга. Её развитие является стратегическим приоритетом для российской образовательной системы, особенно в контексте стабилизации индекса цифровой грамотности, что подчеркивает необходимость внедрения инновационных подходов. Анализ современных инициатив, таких как "Урок Цифры" и "ИТ-диктант", а также данных о региональных и демографических диспропорциях, подтверждает важность дифференцированного подхода к обучению, включая интеграцию искусственного интеллекта и ежегодную актуализацию программ. Предложенные методы формирования и оценки компетенций, адаптированные к различным возрастным группам, подчеркивают необходимость системной работы, охватывающей как школьников, так и взрослых. Дальнейшие исследования должны сосредоточиться на разработке региональных моделей обучения и углубленной интеграции передовых технологий, что обеспечит устойчивое развитие цифрового общества и повышение его конкурентоспособности в условиях эволюции киберугроз.

## СПИСОК ЛИТЕРАТУРЫ

1. Иванченко Д.А., К вопросу формирования и оценки цифровой грамотности личности // Проблемы современного образования, № 3, 2020, С. 66-74.
2. Индекс цифровой грамотности-2024: цифровая грамотность россиян не растет третий год подряд [Электронный ресурс] // Аналитический центр НАФИ. – 2025. – URL: <https://nafi.ru/analytics/index-tsifrovoy-gramotnosti-2024-tsifrovaya-gramotnost-rossiyan-ne-rastet-tretyi-god-podryad/> (дата обращения: 28.08.2025).
3. Жумашева С.С., Цифровая грамотность как одна из ключевых компетенций современного педагога // Вестник науки и образования, № 9-3 (112), 2021, С. 73-77.
4. Захарова А.С., К вопросу о цифровой грамотности студентов // Скиф. Вопросы студенческой науки, № 6 (82), 2023, С. 120-124.
5. Кайсина А.В., Цифровая грамотность как жизненно важный навык школьников в цифровой образовательной среде // Царскосельские чтения, Вып. 2, 2024, С. 348-352.
6. Рогозин С.А., Корчемкина Ю.В., Рузаков А.А., Пути повышения цифровой грамотности будущих педагогов при работе в социальных сетях // Вестник Южно-Уральского государственного гуманитарно-педагогического университета, № 4 (170), 2022, С. 157-170.
7. Ображей О.Н., Цифровая грамотность как императив успешной жизнедеятельности в современном обществе: социологический анализ // Социологический альманах, № 15, 2024, С. 262-272.
8. Урок Цифры — всероссийский образовательный проект в сфере цифровых технологий [Электронный ресурс] // Урок Цифры. – 2025. – URL: <https://урокцифры.рф/> (дата обращения: 14.09.2025).
9. Кибербезопасность 2025: актуальные риски и тренды [Электронный ресурс] // Сибирское представительство издательского дома «Коммерсантъ». – 2025. – URL: [https://events.kommersant.ru/nov/events/2025-04-29\\_kiberbezopasnost-2025-aktualnye-riski-i-trendy/](https://events.kommersant.ru/nov/events/2025-04-29_kiberbezopasnost-2025-aktualnye-riski-i-trendy/) (дата обращения: 20.08.2025).
10. Для школьников стартовал новый сезон проекта «Цифровой ликбез» [Электронный ресурс] // egov-buryatia.ru. – 2025. – URL: [https://egov-buryatia.ru/press\\_center/news/detail.php?ID=196008](https://egov-buryatia.ru/press_center/news/detail.php?ID=196008) (дата обращения: 19.09.2025).
11. Минцифры России объявило о проведении Всероссийской образовательной акции по проверке уровня цифровой грамотности «ИТ-диктант» [Электронный ресурс] // Министерство цифрового развития Республики Дагестан. – 2025. – URL: <https://dagestan.digital/news/mincifry-rossii-obieciavilo-o-provedenii-vserossiiskoi-obrazovatelnoi-akcii-po-proverke-urovnia-cifrovoi-gramotnosti-it-diktant> (дата обращения: 20.09.2025).
12. Выпуск № 2 (2025) журнала: ВОПРОСЫ БЕЗОПАСНОСТИ [Электронный ресурс] // SciNetwork. – 2025. – URL: <https://scinetwork.ru/issues/3102> (дата обращения: 23.09.2025).
13. Цифровую грамотность россиян повысят [Электронный ресурс] // pobedarf.ru. – 2025. – URL: <https://pobedarf.ru/2025/04/03/czifrovuyu-gramotnost-rossiyan-povyssyat/> (дата обращения: 08.08.2025).
14. АНО «Цифровая экономика» представила результаты аналитического отчета «Цифровая грамотность в регионах» [Электронный ресурс] // d-economy.ru. – 2025. – URL: <https://d-economy.ru/news/ano-cifrovaja-jekonomika-predstavila-rezultaty-analiticheskogo-otcheta-cifrovaja-gramotnost-v-regionah/> (дата обращения: 08.09.2025).

УДК 004

## ОБРАБОТКА ДАННЫХ С БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Грачев Александр Михайлович

Военно-медицинская академия имени С. М. Кирова Министерства обороны Российской Федерации

Академика Лебедева ул., 6, лит. Ж, Санкт-Петербург, 194044, Россия

e-mail: gam1404@mail.ru

**Аннотация.** В настоящее время развитие беспилотных летательных аппаратов требует соблюдение информационной безопасности в рамках передачи видеоизображений. В сложившихся условиях необходимо применять комплексный подход, позволяющий учитывать различные факторы, такие как сложившаяся обстановка, временной диапазон и направление применения по назначению.

**Ключевые слова:** информационная безопасность; беспилотные летательные аппараты; обработка изображений; защита данных; киберугрозы.

## PROCESSING DATA FROM UNMANNED AERIAL VEHICLES

Grachev Alexander

S. M. Kirov Military Medical Academy of the Ministry of Defense of the Russian Federation

6 Akademika Lebedeva St., lit. Zh, St. Petersburg, 194044, Russia

e-mail: gam1404@mail.ru

**Abstract.** Currently, the development of unmanned aerial vehicles requires compliance with information security in the context of video transmission. In the current conditions, it is necessary to apply a comprehensive approach that allows taking into account various factors, such as the current situation, time range and intended use.

**Keywords:** information security; unmanned aerial vehicles; image processing; data protection; cyber threats.

Современные технологии применения беспилотных летательных аппаратов (БПЛА) требует комплексного подхода, охватывающего различные направления жизнедеятельности человечества, но особо острыми становятся вопросы передачи информации и её шифрования [1].

Одним из наиболее распространенных рисков является перехват данных, передаваемых между БПЛА и наземной станцией управления. Злоумышленники могут использовать различные методы, такие как перехват Wi-Fi сигнала или радиочастотное сканирование, для получения доступа к изображениям, видео и телеметрической информации. Эти данные могут быть использованы для дезинформации, шантажа или проведения целевых атак.

Несанкционированный доступ к управлению БПЛА представляет собой еще одну серьезную угрозу. Злоумышленники, получив контроль над БПЛА, могут использовать его для нанесения вреда, проведения

разведки или сбора конфиденциальной информации. Подмена изображений, полученных с БПЛА, также является потенциальным риском. Злоумышленники могут заменить реальные данные фальсифицированными, чтобы ввести в заблуждение заинтересованные стороны или скрыть незаконную деятельность. Кроме того, необходимо проводить обучение персонала основам ИБ и разработать планы реагирования на инциденты, связанные с нарушением безопасности данных [2].

Обеспечение информационной безопасности при обработке данных с БПЛА требует комплексного подхода, включающего современные технологии шифрования, защищенные каналы связи и подготовку специалистов. Внедрение комплексных мер позволит повысить надежность систем мониторинга и минимизировать риски [3].

Важным аспектом является защита от несанкционированного доступа к данным, как на этапе передачи, так и при хранении. Необходимо внедрять многофакторную аутентификацию и ролевую модель доступа, чтобы ограничить круг лиц, имеющих возможность взаимодействовать с конфиденциальной информацией. Регулярный аудит безопасности, включающий анализ уязвимостей и тестирование на проникновение, поможет выявить и устранить потенциальные бреши в системе защиты [4].

Не менее значимым является обеспечение физической безопасности оборудования, используемого для обработки данных с БПЛА. Это включает в себя защиту станций управления, серверов и носителей информации от кражи, повреждений и несанкционированного доступа. Необходимо разрабатывать планы реагирования на инциденты, которые позволят оперативно восстановить работоспособность системы в случае возникновения чрезвычайных ситуаций.

Особое внимание следует уделить защите каналов связи, используемых для передачи данных между БПЛА и наземной станцией. Использование защищенных протоколов, шифрование трафика и постоянный мониторинг сети помогут предотвратить перехват и модификацию данных. Необходимо регулярно обновлять программное обеспечение и прошивки оборудования, чтобы устранить известные уязвимости.

Эффективное обеспечение информационной безопасности при обработке данных с БПЛА требует постоянного совершенствования и адаптации к новым угрозам. Необходимо проводить регулярное обучение персонала, чтобы повысить их осведомленность в области информационной безопасности и научить их распознавать и предотвращать атаки.

Внедрение системы мониторинга и анализа событий безопасности позволит оперативно выявлять и реагировать на возникающие угрозы [5].

Важным элементом стратегии защиты данных является разработка и внедрение строгих политик и процедур, регламентирующих все этапы работы с информацией, начиная от ее сбора и обработки, заканчивая хранением и уничтожением. Эти политики должны четко определять роли и обязанности каждого сотрудника, имеющего доступ к данным, а также устанавливать правила поведения в различных ситуациях, связанных с информационной безопасностью.

Для обеспечения соответствия требованиям законодательства и отраслевым стандартам необходимо проводить регулярную оценку рисков и разрабатывать планы по их минимизации. Это позволит своевременно выявлять потенциальные угрозы и принимать меры для их предотвращения. Важно также учитывать специфику использования БПЛА в различных сферах деятельности и адаптировать меры безопасности к конкретным условиям.

В условиях быстро меняющегося ландшафта киберугроз необходимо постоянно совершенствовать систему защиты информации, используя современные технологии и методы. К ним относятся системы обнаружения и предотвращения вторжений, средства защиты от вредоносного программного обеспечения, инструменты анализа трафика и мониторинга событий безопасности. Важно также активно сотрудничать с другими организациями и экспертами в области информационной безопасности для обмена опытом и информацией об угрозах.

Создание эффективной системы информационной безопасности при обработке данных с БПЛА — это непрерывный процесс, требующий постоянного внимания и инвестиций. Только комплексный подход, включающий организационные, технические и кадровые меры, позволит обеспечить надежную защиту конфиденциальной информации и предотвратить несанкционированный доступ к ней.

#### СПИСОК ЛИТЕРАТУРЫ

1. Грачев, А. М. Подготовка будущих кадров по управлению беспилотными летательными аппаратами / А. М. Грачев // Информационная безопасность регионов России (ИБРР-2023). СПб., 2023. С. 308-309.
2. Balog, M. Human capital in the digital economy as a factor of sustainable development / M. Balog, S. Demidova, N. Lesnevskaya // Sustainable Development and Engineering Economics. 2022. No. 1(3). P. 47-60. DOI 10.48554/SDEE.2022.1.3.
3. Еремина, И. В. Человеческий капитал как фактор обеспечения экономической и кадровой безопасности в организации / И. В. Еремина // Инновационное развитие экономики. 2021. № 1(61). С. 303-305. DOI 10.51832/2223-7984\_2021\_1\_303.
4. Грачев, М. И. Человеческий фактор в принятии управленческих решений / М. И. Грачев, В. Г. Бурлов // T-Comm: Телекоммуникации и транспорт. 2024. Т. 18, № 3. С. 27-33. DOI 10.36724/2072-8735-2024-18-3-27-33.
5. Грачев, М. И. Обеспечение информационной безопасности предприятия / М. И. Грачев, Н. Г. Грачева // Региональная информатика и информационная безопасность: Сборник трудов Санкт-Петербургской международной конференции, Санкт-Петербург, 25–27 октября 2023 года. Санкт-Петербург: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2023. С. 68-71. EDN FRSTFJ.



УДК 37

**ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ В МУЗЫКАЛЬНО-ТВОРЧЕСКОЙ ДЕЯТЕЛЬНОСТИ С ИСПОЛЬЗОВАНИЕМ КЛАВИШНОГО СИНТЕЗАТОРА****Давлетова Клара Борисовна, Романова Наталия Александровна**

Российский государственный педагогический университет им. А. И. Герцена

наб. реки Мойки, д. 48, 191186, Санкт-Петербург, Россия

Центр творческого развития и гуманитарного образования детей «На Васильевском»

Василеостровского района Санкт-Петербурга

Наличная ул., 55, Санкт-Петербург, 199406, Россия

e-mails: klarad@list.ru, vna06@ya.ru

**Аннотация.** Обеспечение информационно-психологической безопасности личности становится актуальной проблемой в связи с тем, что жизнедеятельность человека осуществляется в развивающейся информационной образовательной среде. В данном случае любые изменения информации и процессов функционирования среды в настоящее время используются социальными субъектами для оказания воздействия на психику людей, манипуляций личностью. Наиболее активно этот процесс может быть проявлен по отношению к детям и подросткам, применяющим информационные технологии в образовательном процессе в том числе. Развитие музыкально-компьютерных технологий и цифровых клавишных синтезаторов, широкое их применение в музыкально-творческой деятельности, ставит актуальными вопросы обеспечения информационно-психологической безопасности современных детей и подростков.

**Ключевые слова:** информационно-психологическая безопасность; учреждение дополнительного образования детей; информационная образовательная среда; музыкальное образование; клавишный синтезатор; музыкально-компьютерные технологии; музыкально-творческая деятельность.

**INFORMATION AND PSYCHOLOGICAL SECURITY IN MUSICAL AND CREATIVE ACTIVITIES USING A KEYBOARD SYNTHESIZER****Davletova Klara, Romanova Natalia**

Herzen State Pedagogical University of Russia

48 Moika Embankment, 191186, St. Petersburg, Russia

Centre for Creative Development and Humanitarian Education of Children «On Vasilyevsky Island»

Vasileostrovsky district of St. Petersburg, 55 Nalichnayastr., St. Petersburg, 199406, Russia

e-mails: klarad@list.ru, vna06@ya.ru

**Abstract.** Ensuring the information and psychological security of a person is becoming an urgent problem due to the fact that human life is carried out in a developing information educational environment. In this case, any changes in information and processes of the functioning of the environment are currently being used by social actors to influence people's psyche and personality manipulation. This process can be most actively manifested in relation to children and adolescents who use information technology in the educational process, including. The development of music and computer technologies and digital keyboard synthesizers, their widespread use in musical and creative activities, raises urgent issues of ensuring the information and psychological safety of modern children and adolescents.

**Keywords:** information and psychological security; institution of additional education for children; information educational environment; music education; keyboard synthesizer; music computer technology musical and creative activities.

Под информационно-психологической безопасностью понимается состояние защищенности отдельных лиц от информационно-психологических воздействий негативного характера и связанных с этим других жизненно важных интересов личности.

В настоящее время возрастает воздействие информационных средств на общественное сознание, в том числе на психику личности. Современные технологии практически неограниченно управляют информационным воздействием на сознание людей. В первую очередь, это касается детей и подростков, которых окружает мир информационных технологий и медиа.

Бурное развитие информационно-коммуникативных технологий и информационной образовательной среды в первом десятилетии XXI века коснулось также системы музыкального образования. Формируется новое звуковое пространство, и музыкально-компьютерные технологии - синтезаторы проникают в разные жанры. Композиторы используют синтезаторы в составе оркестров, появляются музыканты - исполнители на клавишных синтезаторах. Появление новых музыкальных инструментов или музыкальных синтезаторов обусловлено двумя основными причинами. Первая из них — стремление музыкантов обогатить палитру своего музыкального творчества. Вторая причина связана с историческим совершенствованием музыкального инструментария, который в своей конструкции стремится опираться на современные достижения науки и техники в области создания звука. Слово «синтезирование» означает создание чего-либо с помощью комбинаций отдельных элементов его составляющих. Синтезированный звук — это звук, который музыкант создает с помощью какого-либо музыкального инструмента из элементов, его составляющих. Синтезированный звук может быть традиционным акустическим музыкальным тембром или похожим на него, либо он может быть также

совершенно новым, не существовавшим ранее, оригинальным. Однако общим для всей синтезированной музыки является то, что звучание «само по себе» не есть музыка, музыка возникает в результате взаимодействия этих звуков и музыканта, который воспроизводит звучание или создает композицию [1].

Успех художественно-творческой деятельности во многом определяется пониманием природы ее инструментария. Каждый музыкальный инструмент обладает особенной индивидуальностью, и овладеть им в совершенстве – значит глубоко проникнуться этой индивидуальностью.

Современный электронный (цифровой) музыкальный инструментарий, созданный на основе быстро развивающихся музыкально-компьютерных технологий (далее – МКТ), и – особенно – клавишный синтезатор как наиболее часто используемый компонент в творчестве композиторов и исполнителей, уверенно занимает медийное пространство, расширяя и обогащая сферы творческой деятельности музыканта за счет многообразия встроенных в функций, разнообразия звуковых красок, возможности звукового синтеза и создания собственных оригинальных тембров [2; 3].

Предъявляя музыканту иные, по сравнению с акустическими инструментами, требования (знания по теории музыки, гармонии, анализу музыкальной формы дополняются знаниями основ композиции и импровизации, звукорежиссуры; также знания в области информатики), цифровой музыкальный синтезатор дает возможность управления функциями МКТ-программ, встроенных в инструмент. При работе с клавишным синтезатором музыкант выступает одновременно в роли исполнителя и композитора, выполняя при этом функции звукорежиссера и пользователя (см. подробнее о функциональных возможностях нового электронного и цифрового музыкально-творческого инструментария в работах [4-6]). Это является основой творческой деятельности на электронных (цифровых) музыкальных синтезаторах: создание оригинальной авторской композиции или аранжировки, которая предполагает добавление авторских элементов в музыкальный материал, изменение фактуры, формы, подбор, обработка или создание собственных тембров и т.д.

Технические возможности клавишного синтезатора, отличающие его от традиционных музыкальных инструментов, открывают большие перспективы в различных областях музыкального воспитания детей. Использование информационных технологий и электронных музыкальных инструментов в учреждении дополнительного образования детей открывает перспективы создания «среды ускоренного музыкального воспитания и развития детей», расширяет ресурсные возможности для работы с педагогами, учащимися, их родителями. Сочетание информационных технологий с академическим музыкальным образованием позволяет разнообразить технологии работы с учебным материалом, вариативно раскрывать материал, связанный с музыкальным искусством рассмотрением стилей, жанров в музыке. В результате содержание материала приобретает новое качество и значение. Такие формы обучения повышают мотивацию, стимулируют самостоятельную деятельность учащегося. Основу обучения на синтезаторах составляет процесс творчески организованной деятельности, способствующей вовлечению обучающихся в создание электронного музыкального проекта, побуждающей к рассуждению, самостоятельному мышлению.

Исследователи в работах подчеркивают, что, благодаря появлению электронных музыкальных инструментов, решается важная педагогическая проблема – приобщение широких масс учащихся к музыкальному творчеству. Использование ЭМИ в музыкальном образовании ставит принципиально новые задачи, создают необходимость поиска новых подходов к организации образовательного процесса, новых технологий и форм музыкального воспитания и развития детей. В учреждениях дополнительного образования детей наблюдается рост популярности электронных (цифровых) музыкальных инструментов, клавишных синтезаторов, которые становятся все более востребованными среди педагогов, детей и их родителей [7-10]. Такая популярность обусловлена новым подходом к музыкальному воспитанию, основанного на специфических возможностях музыкально-компьютерного инструментария:

- многофункциональность;
- программируемость – возможность создания предварительного музыкального материала, его запись, сохранение и использование при необходимости в процессе исполнения;
- многотембровость;
- использование встроенного секвенсора;
- возможность создания, записи и сохранения музыкального материала;
- функции хранения музыкальной информации и создания пользовательских настроек;
- и мн. др. (см., например, в работе [8]).

Обучение в классе клавишного синтезатора реализуется через современные педагогические технологии: индивидуальный и личностно-деятельностный подходы; включение игровых, информационно-коммуникационных технологий и МКТ; из педагогических инноваций необходимо выделить также интеграцию музыкальной педагогики и цифровых технологий, а также использование специфических приемов работы с интерфейсом электронного (цифрового) музыкального инструмента.

Обращение к музыкально-компьютерным технологиям, занятие художественным творчеством на электронных (цифровых) музыкальных инструментах, в том числе – клавишных синтезаторах дает возможность по-новому строить музыкальное образование [11-13]. Систематизация и углубление знаний обучающихся при выполнении заданий из области разных предметов позволяет использовать новые приемы работы с информацией: перенос ранее пройденных действий на другое содержание, осознание взаимосвязи различных предметных областей. При таком подходе повышается качество учебного процесса: развивается и

активизируется мыслительная и познавательная деятельность; расширяются представления о целостности мира; формируется успешность как качество личности учащегося. Учебно-методический комплекс сопровождения программы включает банк дидактических материалов: авторские учебно-методические пособия; методические разработки педагогов; электронные учебники и разработки; работу с музыкальными сайтами, в том числе и с официальным сайтом Yamaha, где есть возможность загружать в синтезатор новые тембры и стили, а также музыкальные файлы.

Основные образовательные результаты обучения по программе:

1. Развитие многогранной музыкальной деятельности, включающей основы исполнительства на музыкальном инструменте; композиторского творчества при работе над аранжировкой музыки; основы звукорежиссуры при работе над балансировкой партий, звуковым синтезом, обработкой звука.

2. Формирование цифровых компетенций и навыков работы с современными технологиями (навыки компьютерного пользователя при записи пользовательских программ, работе с секвенсором, музыкальными файлами, внешними устройствами и др.).

3. Создание медийных продуктов – авторских аранжировок, музыкальных композиций, запись и сохранение в аудиобиблиотеках детских творческих работ.

4. Развитие творческой индивидуальности учащегося (средства выразительности для раскрытия музыкального образа и осуществления замысла проекта учащийся подбирает сам, что дает возможность каждому ощутить свою творческую уникальность и индивидуальность).

5. Гармоничное развитие личности учащегося через интеграцию музыкально-творческой деятельности.

За последнее десятилетие увеличилось количество исследований в области информационно-психологической безопасности личности и влияния информационных технологий на сознание человека. Исследователи отмечают, что большой объем информации, развитие технологий накладывает отпечаток на внутренний и внешний мир человека. Эти факты отражаются на уровне информационной безопасности и защищенности. Потребность в безопасности является одной из базовых потребностей личности, связанная с отсутствием опасности.

Таким образом, информационно-психологическую безопасность личности определяют как способ организации и развития жизнедеятельности, при котором личность может защитить себя при информационном воздействии.

Так, Лунев А.Н. и Пугачева А.И. выделяют следующие критерии информационно-психологической безопасности личности [13]:

доступность - возможность реализовывать информационные права и свободы;

– пертинентность - содержание информационных потребностей и степень их удовлетворения; интерес к различным источникам информации и связанные с ними ожидания;

– ценность - осознание влияния информационных процессов и технологий на развитие личности, общества; информированность об информационно-психологических опасностях и угрозах; признание приоритета информационно-психологической безопасности личности; устойчивая направленность на освоение механизмов информационно-психологической самозащиты; отношение индивида к личной безопасности как к общественному благу;

– адекватность - целостное представление об информационной сфере деятельности; способность давать субъективную оценку ситуации как потенциально опасной; информационно-компьютерная грамотность;

– защищенность - освоение механизмов противодействия негативным информационным воздействиям.

Обеспечение информационно-психологической безопасности образовательно-воспитательного процесса является одним из важных аспектов при обучении детей музыке с использованием цифровых клавишных синтезаторов. Данное положение, которое включает в себя: формирование осознанного использования технологий; сохранение необходимого творческого баланса между цифровыми технологиями и музицированием на акустических инструментах; соблюдение техники безопасности при работе с синтезатором, электронной аппаратурой; обеспечение психолого-педагогического сопровождения творческого и образовательного процесса; создание условий для раскрытия его индивидуальности и развития творческих способностей.

#### СПИСОК ЛИТЕРАТУРЫ

1. Горбунова И.Б. Музыкально-компьютерные технологии как новая обучающая и творческая среда // Современное музыкальное образование – 2002. Материалы Международной научно-практической конференции. Российский государственный педагогический университет им. А. И. Герцена, Санкт-Петербургская государственная консерватория им. Н. А. Римского-Корсакова / Под общ. ред. И. Б. Горбуновой. СПб., 2002. С. 161-169.
2. Gorbunova I.B., Davletova K.B. Information Educational Environment as a Resource for Advancing a Teacher-Musician's Skills in the Additional Children Education System. Revista Conrado. 2020. V. 16. No. 74. Pp. 38-44.
3. Белов Г.Г., Горбунова И.Б. Электроника в музыкальном искусстве: влечение времени // Мир науки, культуры, образования. 2020. № 5 (84). С. 207-210.
4. Горбунова И.Б. Компьютерная студия звукозаписи как инструмент музыкального творчества и феномен музыкальной культуры // Общество: философия, история, культура, 2017. № 2. С. 87-92.
5. Горбунова И.Б. Информационные технологии в музыке. Т. 1: Архитектоника музыкального звука: учебное пособие. СПб.: Изд-во РГПУ им. А. И. Герцена, 2009. 175 с.
6. Горбунова И.Б. Информационные технологии в музыке. Т. 2: Музыкальные синтезаторы: учебное пособие. СПб.: Изд-во РГПУ им. А.И. Герцена, 2010. 205 с.
7. Горский В.А., Журкина А.А. Педагогические принципы развития системы дополнительного образования // Дополнительное образование, 1999. №2. С. 4-6.

8. Горбунова И.Б., Алиева И.Г. О проекте создания интеллектуальной системы по каталогизации и анализу музыки народов мира // Общество: философия, история, культура. 2016. № 9. С. 105-108.
9. Горбунова И.Б., Давлетова К.Б. Электронные музыкальные инструменты в системе общего музыкального образования // Теория и практика общественного развития, 2015. № 12. С. 411-415.
10. Давлетова К.Б. Информационная образовательная среда курсов повышения квалификации педагога-музыканта (секция «Электронные музыкальные инструменты») // Мир науки, культуры, образования. 2021. № 3 (88). С. 335-338.
11. Красильников И.М. Музыкальное искусство и образование XXI века // Сборник материалов международной научно-практической конференции «Современное музыкальное образование – 2010» / Под общ. ред. И. Б. Горбуновой. СПб.: Изд-во «Лема», 2011. С. 22-28.
12. Красильников И.М. Педагогика цифровых искусств – новое направление развития теории и практики художественного образования // Проблемы современного образования. 2011. № 6. С. 11-123.
13. Лунев А.Н., Пугачев Н.Б., Стуколова Л.З. Информационно-психологическая безопасность личности: сущностная характеристика // Современные проблемы науки и образования. 2014. №1.; URL: <https://science-education.ru/ru/article/view?id=11882> (дата обращения: 30.09.2025).

УДК: 004.056

## **ИНТЕГРАЦИЯ САУНД-ДИЗАЙНА В ОБРАЗОВАТЕЛЬНЫЕ ПРОГРАММЫ: КОЛЛЕКТИВНОЕ ЦИФРОВОЕ ТВОРЧЕСТВО И СОЦИОКОМПЬЮТИНГ**

**Дельцова Наталья Сергеевна**

Российский государственный педагогический университет им. А. И. Герцена,  
реки Мойки наб., 48, Санкт-Петербург, 191186, Россия  
e-mail: gorbunovaib@herzen.spb.ru.

**Аннотация.** В статье рассматривается проблема интеграции саунд-дизайна в мультимедийные образовательные программы для дошкольников в контексте цифровой трансформации образования. Особое внимание уделяется феномену коллективного саунд-дизайна и социокompьютинга — процессам совместного создания и переработки звукового контента в онлайн-сообществах. Автор анализирует возможности применения практик цифрового коллективного творчества в дошкольной педагогике, показывая, что использование звука в образовательной среде не только усиливает когнитивное и эмоциональное развитие детей, но и формирует предпосылки для их включения в цифровую культуру будущего.

**Ключевые слова:** саунд-дизайн; дошкольное образование; мультимедийные материалы; музыка как коммуникация; социокompьютинг; коллективное творчество; медиаграмотность.

## **INTEGRATION OF SOUND DESIGN IN TO EDUCATIONAL PROGRAMS: COLLECTIVE DIGITAL CREATIVE WORK AND SOCIO COMPUTING**

**Deltsova Natalia**

Herzen State Pedagogical University of Russia, St. Petersburg  
48 Moika River Emb., St. Petersburg, 199406, Russia  
e-mail: gorbunovaib@herzen.spb.ru.

**Abstract.** The article examines the problem of integrating sound design into multimedia educational programs for preschoolers in the context of digital transformation of education. Special attention is paid to the phenomenon of collective sound design and sociocomputing — the processes of joint creation and processing of sound content in online communities. The author analyzes the possibilities of applying digital collective creative work practices in preschool pedagogy, showing that the use of sound in an educational environment not only enhances the cognitive and emotional development of children, but also forms the prerequisites for their inclusion in the digital culture of the future.

**Keywords:** sound design; preschool education; multimedia materials; music as communication; sociocomputing; collective creativity; media literacy.

Современное образование находится в условиях активной цифровой трансформации, что требует новых подходов к разработке учебных материалов для детей дошкольного возраста. Одним из перспективных направлений становится интеграция саунд-дизайна в мультимедийные образовательные программы. Звуковая среда при этом играет не только декоративную или иллюстративную роль, но и становится самостоятельным инструментом формирования когнитивных, эмоциональных и коммуникативных навыков. Параллельно с этим в культуре развивается феномен коллективного саунд-дизайна, связанный с деятельностью онлайн-сообществ, где пользователи создают, перерабатывают и распространяют звуковой контент, превращая музыку и звук в формы цифровой коммуникации. Эти два направления — педагогическая интеграция звука и социокompьютинг — пересекаются и могут взаимно обогащать друг друга, открывая новые перспективы как для образования, так и для культуры в целом.

*Саунд-дизайн в образовательных мультимедиа для дошкольников.* В дошкольном возрасте звук является мощным инструментом развития ребёнка, так как именно в этот период формируются основы восприятия мира, эмоциональной отзывчивости и когнитивных навыков. Включение саунд-дизайна в мультимедийные образовательные материалы позволяет существенно обогатить процесс обучения. Звуковые эффекты, музыкальные фрагменты и специально подобранные шумы помогают детям формировать устойчивые

ассоциативные связи и облегчать запоминание информации. Помимо этого, звук усиливает эмоциональное вовлечение: динамичные сигналы стимулируют внимание, а спокойное музыкальное сопровождение помогает удерживать концентрацию на учебных заданиях или сюжетах.

Особое значение имеет возможность для ребёнка активно участвовать в создании звуковой среды. Задания, предполагающие озвучивание персонажей, подбор звуковых эффектов к картинке или создание «коллажа» из шумов, превращают обучение в творческий процесс. Такие практики развивают слуховую память, внимание к деталям, воображение и креативность. Звук в этом случае становится не просто фоном, а средством формирования многосенсорного восприятия, которое обеспечивает более глубокое усвоение знаний и одновременно расширяет творческие возможности ребёнка. (Отметим, в частности, что на таком подходе основана разработка интеллектуальной системы каталогизации музыки народов России и мира (см. подробнее в работах [1, 2]), создаваемая сотрудниками научно-методической лаборатории «Музыкально-компьютерные технологии» Российского государственного университета им. А. И. Герцена).

*Музыка как цифровая коммуникация: социокomпьютинг и коллективное творчество.* В цифровую эпоху музыка и звук выходят за рамки традиционного понимания искусства и становятся средствами коммуникации и коллективного творчества [3].

С развитием онлайн-платформ, таких как SoundCloud, BandLab, TikTok или Discord, пользователи получили возможность не только слушать, но и создавать, редактировать и перерабатывать аудиоконтент в открытой среде. Этот процесс получил название «социокomпьютинг» и представляет собой форму цифрового взаимодействия, где звук используется как медиатор общения и культурного обмена [4, 5].

Звуковые объекты в таких сообществах редко воспринимаются как окончательные. Напротив, они становятся материалом для бесконечных ремиксов, дополнений и переосмыслений. Пользователи взаимодействуют друг с другом через обмен файлами, комментарии и совместные проекты, создавая условия для горизонтального обучения и обмена опытом. Ценность в этой системе заключается не только в конечном результате, но и в самом процессе взаимодействия. Музыка и звук выполняют функцию социальной связки, укрепляя чувство принадлежности к сообществу и формируя новые культурные идентичности.

*Пересечение подходов: от дошкольного образования к цифровым сообществам.* Опыт коллективного саунд-дизайна в цифровых сообществах [6; 7] может быть адаптирован для использования в дошкольном образовании, создавая тем самым мост между ранними образовательными практиками и будущим включением детей в цифровую культуру.

Образовательные программы могут заимствовать модель совместного творчества, где дети, педагоги и родители вместе создают звуковые библиотеки для мультимедийных материалов, записывают природные шумы или озвучивают сказочные сюжеты. Такая деятельность развивает у ребёнка умение вносить свой вклад в общее дело, воспринимать и дополнять работу других, а также понимать ценность коллективного результата.

Кроме того, подобные практики способствуют развитию ранней медиаграмотности. Ребёнок учится воспринимать цифровой контент как изменяемый и поддающийся переработке, что формирует критическое отношение к медиа и подготавливает к участию в цифровой культуре. Игровые формы коллективной работы со звуком становятся не только средством обучения, но и подготовкой к будущим формам социального взаимодействия, основанным на творчестве и сотрудничестве.

Таким образом, интеграция принципов социокomпьютинга в дошкольные образовательные программы позволяет не только повысить их эффективность, но и расширить горизонты воспитания, сделав звук универсальным посредником между обучением и цифровой культурой.

Интеграция саунд-дизайна в образовательные мультимедиа для дошкольников является эффективным способом усиления когнитивного и эмоционального развития ребёнка [7, 8]. Однако её значение выходит за пределы педагогики в узком смысле. Опыт цифровых сообществ, где звук используется как форма коммуникации и коллективного творчества, демонстрирует новые перспективы, которые можно перенести в образовательный процесс.

Таким образом, работа со звуком в дошкольном возрасте становится не только методом обучения, но и инструментом социализации, подготавливающим ребёнка к участию в цифровой культуре будущего.

#### СПИСОК ЛИТЕРАТУРЫ

1. Горбунова И.Б., Алиева И.Г. О проекте создания интеллектуальной системы по каталогизации и анализу музыки народов мира // Общество: философия, история, культура. 2016. № 9. С. 105-108.
2. Горбунова И.Б., Алиева И.Г. К проблематике разработки интеллектуальной системы каталогизации музыки народов России и мира. Трансдисциплинарный подход к изучению музыкальных явлений: теория нечётких множеств // Региональная информатика и информационная безопасность. Сборник трудов Санкт-Петербургской международной конференции и Санкт-Петербургской межрегиональной конференции. Санкт-Петербург, 2024. С. 316-319.
3. Jenkins H. Convergence Culture: Where Old and New Media Collide. New York: NYU Press, 2006.
4. Turkle S. Alone Together: Why We Expect More from Technology and Less from Each Other. Basic Books, 2011.
5. Brown A. R. Music and Digital Culture: From Creative Practice to Socio-Computing. Routledge, 2015.
6. Гребенщикова Т.А. Саунд-дизайн как инструмент образовательной среды // Педагогика искусства. 2020. № 4.
7. Литвинова Т.Н. Цифровая коммуникация и коллективное творчество в образовательных практиках // Вопросы образования. 2021. № 2.
8. Чумакова Н.В. Медиаграмотность в дошкольном образовании: подходы и перспективы // Современное дошкольное образование. 2022. № 1.

УДК: 004.056

**ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МУЗЫКАЛЬНОМ ОБРАЗОВАНИИ****Денисова Ольга Сергеевна**

Российский государственный педагогический университет им. А. И. Герцена  
реки Мойки наб., 48, Санкт-Петербург, 191186, Россия  
Открытая (сменная) общеобразовательная школа г. Онеги  
Пр. Гагарина, 48, г. Онега, Архангельская область, 164840, Россия  
e-mail:olganum@gmail.com

**Аннотация.** В статье рассматривается проблема информационной безопасности в обучении, в частности музыкальном. С развитием информационных технологий музыкальное образование для детей всё больше перемещается в онлайн-пространство. Определены основные риски и угрозы информационной безопасности, способы защиты от информационных угроз. Подчеркнута связь информационной безопасности с психологической.

**Ключевые слова:** информационная безопасность, онлайн-пространство, кибербуллинг, персональные данные, цифровизация, фишинг.

**ENSURING INFORMATION SECURITY IN MUSIC EDUCATION****Denisova Olga**

A. I. Herzen State Pedagogical University of Russia  
Moika River Embankment, 48, St. Petersburg, 191186, Russia  
Onega Open (Shift) Comprehensive School  
Gagarin Ave., 48, Onega, Arkhangelsk Region, 164840, Russia  
e-mail:olganum@gmail.com

**Abstract.** The article addresses the problems of information security in education, in particular music. With the development of information technology, music education for children is increasingly moving into the online space. The main risks and information security, methods of protection against information threats are identified. The connection between information security and psychological security is emphasized.

**Keywords:** information security, online space, cyberbullying, personal data, digitalization, phishing.

Современное образование невозможно представить без активного использования информационных технологий. С их развитием музыкальное образование для детей всё больше перемещается в онлайн-пространство. Использование интернета для занятий музыкой, обмена материалами и участия в конкурсах открывает перед учащимися новые возможности, но также ставит перед образовательными учреждениями и родителями важные задачи по обеспечению информационной безопасности.

В условиях пандемии и растущей популярности дистанционного обучения дети всё чаще используют онлайн-платформы для занятий музыкой. Такие платформы могут быть подвержены кибератакам, фишингу и другим угрозам, что создаёт опасность для конфиденциальности и безопасности данных.

Пользование интернетом несет за собой такие риски как зависимость от компьютера, компьютерная тревожность (не редко сопровождаемая стрессом), технократизация мышления [1, 37].

В музыкальном образовании дети часто участвуют в онлайн-форумах, социальных сетях и конкурсах, где могут столкнуться с кибербуллингом, мошенничеством или контактами с подозрительными лицами. Недостаток контроля и модерации на таких площадках может привести к негативным последствиям.

Как и в любой другой образовательной среде, в музыкальных школах собирается множество персональных данных детей и их родителей: имена, адреса, контакты, академические достижения и многое другое. В случае утечки этих данных существует риск их неправомерного использования, что может привести к негативным последствиям для детей и их семей. Музыкальные педагоги и родители не всегда обладают достаточными знаниями в области информационной безопасности. Это может привести к недостаточной защите используемых программ и устройств, а также к уязвимости данных.

Для обеспечения информационной безопасности важно проводить регулярные занятия по информационной безопасности, где детям и их родителям объясняют, как защитить свои данные в интернете, как распознавать угрозы и какие действия предпринимать в случае подозрения на нарушение безопасности.

Выбор онлайн-платформ для музыкального образования должен основываться на их репутации и уровне безопасности. Необходимо выбирать те сервисы, которые обеспечивают защиту данных, используют шифрование и предлагают многофакторную аутентификацию.

Организаторы онлайн-конкурсов и образовательных платформ должны обеспечивать модерацию общения, чтобы защитить детей от нежелательных контактов и контента. Родители также должны контролировать, с кем общаются их дети в интернете и на каких платформах они проводят время.

Педагоги и родители должны следить за тем, чтобы все устройства, используемые для обучения, были защищены антивирусными программами и регулярными обновлениями систем безопасности. Это минимизирует риски заражения вредоносными программами.

Информационная безопасность тесно переплетается с психологией. Психологическая безопасность «определяет динамическое равновесие между человеком и социальной средой в сторону повышения психического здоровья личности.... Потребность в безопасности доминирует в ситуациях напряженных, побуждая человека мобилизовать все силы на борьбу с угрозой, а не на обучение» [2, 149].

Информационная безопасность в детском музыкальном образовании требует комплексного подхода, включающего в себя технические меры, обучение детей и родителей, а также контроль и модерацию онлайн-активности. В условиях растущей цифровизации образования важно создать безопасную среду, где дети смогут развивать свои таланты, не подвергаясь рискам и угрозам, связанным с использованием современных технологий. Только совместные усилия педагогов, родителей и самих учащихся могут обеспечить надежную защиту данных и комфортное обучение в цифровом пространстве. Учащиеся уже на ранних этапах обучения должны знакомиться с тем, как обезопасить себя и решать проблемы с кибербезопасностью, знать какую информацию можно доверять собственным гаджетам и какие сайты можно посещать [3, 37]. В современном мире «информационная безопасность – важнейший компонент национальной безопасности, информационная безопасность становится одним из элементов национальной, общественной и личной безопасности» [4].

#### СПИСОК ЛИТЕРАТУРЫ:

1. Зубалова О. А. Проблемы информационной безопасности образовательной среды в современных условиях [Электронный ресурс] // Научная электронная библиотека «КиберЛенинка» – URL: <https://cyberleninka.ru/article/n/problemny-informatsionnoy-bezopasnosti-obrazovatelnoy-sredy-v-sovremennyh-usloviyah> (дата обращения: 21.08.2024). С. 36-38.
2. Баева И. А. Психологическая безопасность в образовании : Монография. – Санкт-Петербург: Издательство «Союз», 2002. 271 с.
3. Зубалова О. А. Проблемы информационной безопасности образовательной среды в современных условиях [Электронный ресурс] // Научная электронная библиотека «КиберЛенинка» – URL: <https://cyberleninka.ru/article/n/problemny-informatsionnoy-bezopasnosti-obrazovatelnoy-sredy-v-sovremennyh-usloviyah> (дата обращения: 21.08.2024). С. 36-38.
4. Собилов М. Ш. Информационные технологии и безопасность среди детей [Электронный ресурс] // ХАБАР / NEWS – URL: <https://www.hgu.tj/news/media/item/595.html> (дата обращения: 21.08.2024).
5. Степанова Т. Ю. Обеспечение информационной безопасности в образовательной организации [Электронный ресурс] // Научная электронная библиотека «КиберЛенинка» – URL: <https://cyberleninka.ru/article/n/obespechenie-informatsionnoy-bezopasnosti-v-obrazovatelnoy-organizatsii> (дата обращения: 21.08.2024).

УДК 004.056.5

### ГЕНЕРАЦИЯ УЧЕБНЫХ МАТЕРИАЛОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПОМОЩЬЮ ЯЗЫКОВЫХ МОДЕЛЕЙ

**Карганов Виталий Вячеславович, Яровой Роберт Владимирович**

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: vitalik210277@mail.ru, Nadzar@yandex.ru

**Аннотация.** Тезис раскрывает методологические принципы генерации интерактивных обучающих сценариев, в которых профессиональные компетенции разворачиваются через сюжет, выбор и симулированное противодействие угрозам.

**Ключевые слова:** языковая модель; информационная безопасность; моделирование сценариев; цифровые угрозы; обучающий агент; нарратив; интерактивное обучение; генерация контента.

### GENERATION OF TRAINING MATERIALS IN THE FIELD OF INFORMATION SECURITY USING LANGUAGE MODELS

**Karganov Vitaly, Yarovoy Robert**

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: vitalik210277@mail.ru, Nadzar@yandex.ru

**Abstract.** The thesis reveals the methodological principles of generating interactive learning scenarios in which professional competencies are developed through plot, choice and simulated counteraction to threats.

**Keywords:** language model; information security; scenario modeling; digital threats; learning agent; narrative; interactive learning; content generation.

Современное образование в области информационной безопасности страдает от дидактической инерции, сводящейся к передаче знаний в отрыве от ситуации применения. Визуальные новеллы — жанр, сочетающий интерактивность, нарративность и вариативность — предоставляют возможность переноса обучающего контента в формат симулированного опыта. Интеграция LLM в процесс создания таких новелл обеспечивает персонализацию, тематическую гибкость и дидактическую насыщенность [1–3].

Ключевые свойства визуальной новеллы — ветвящийся сюжет, выбор, эмоциональное вовлечение — создают среду, в которой усвоение понятий ИБ происходит не декларативно, а через действие, рефлексии и последствия. Элементы угроз, инцидентов, уязвимостей инкапсулируются в сценарии, где игрок становится агентом, а сюжет — пространством профессионального моделирования. Поведенческие ошибки фиксируются, анализируются и повторно проигрываются без ущерба для реальной инфраструктуры.

Большая языковая модель встраивается в архитектуру генерации: сюжет, главы, сцены, диалоги, визуальный ряд. Эвристики включения учебного материала опираются на три принципа:

- обучение через ситуацию: пользователь интерпретирует инцидент, применяя знания;
- обучение через противника: демонстрируются действия атакующего;
- обучение через последствия: сцена разворачивается в зависимости от предпринятых шагов [4–5].

Уникальность подхода — в трансляции понятий через драматургию. Проверка знания многофакторной аутентификации может реализовываться как сценический выбор, не нуждающийся в пояснении. Дозировка сложности осуществляется через реплики, рассуждения, наглядность и контекст. Модель формирует материал, соответствующий психолингвистическим особенностям целевой аудитории и тематике угроз.

Заключительный эффект — формирование обучающей среды, в которой знания и действия соотносятся в режиме когнитивной симуляции. Визуальная новелла, созданная LLM, становится лабораторией нарративного эксперимента, где происходит не запоминание, а проживание.

#### СПИСОК ЛИТЕРАТУРЫ

1. Карганов В.В., Федоров П.Н., Яшин В.И. Альтернативный подход по обучению специалистов в области защиты информации // Сборник избранных статей по материалам научных конференций ГНИИ «Нацразвитие». Санкт-Петербург, 2021. С. 375-382.
2. Карганов В.В., Федосеев Д.О., Карганова А.И. Применение инновационных технологий в системе военного профессионального образования // Инновационная деятельность в Вооруженных Силах Российской Федерации. Труды всеармейской науч.-практ. конф. 2019. С. 14-17.
3. Яровой Р.В. Роль искусственного интеллекта в персонализации образования // Региональная информатика и информационная безопасность. Сборник трудов Санкт-Петербургской международной конференции и Санкт-Петербургской межрегиональной конференции. Санкт-Петербург, 2024. С. 389-393.
4. Чувилов Д.А., Ким Р.И., Балдин А.В., Адамова Л.Е. Анализ больших языковых моделей для построения диалоговых систем // МИВАР'24. Сборник научных статей. Москва, 2024. С. 426-431.
5. Макаров О.Б. Использование современных больших языковых моделей с целью получения новых знаний // Инициативы молодых — науке и производству. Сборник статей VI Всероссийской научно-практической конференции молодых ученых и студентов. Пенза, 2023. С. 545-549.

УДК 004.056; 343.721

#### РАЗРАБОТКА КУРСА «ПРИЕМЫ РАСПОЗНАВАНИЯ И МЕРЫ ЗАЩИТЫ ОТ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА» ДЛЯ ПЕРЕПОДГОТОВКИ КАДРОВ ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЙ

Ковганко Валерия Егоровна

Санкт-Петербургский университет промышленных технологий и дизайна

Большая Морская ул., 18, Санкт-Петербург, 191186, Россия

e-mail: KovLerEgo-student@ya.ru

**Аннотация.** Поднимается вопрос о необходимости введения курса повышения квалификации сотрудников образовательных учреждений с целью привлечь внимание к участвовавшим случаям телефонного мошенничества и распространения информации о приемах и мерах защиты от мошенников среди обучающихся. Важным становится повышение финансовой и правовой грамотности населения.

**Ключевые слова:** повышение квалификации; мошенничество; киберугрозы; социальный инжиниринг; схемы мошенничества; меры защиты от мошенников; подготовка кадров.

#### DEVELOPMENT OF THE COURSE «RECOGNITION TECHNIQUES AND MEASURES TO PROTECT AGAINST TELEPHONE FRAUD» FOR RETRAINING PERSONNEL IN EDUCATIONAL INSTITUTIONS

Kovganko Valeria

Saint Petersburg State University of Industrial Technologies and Design

18 Bolshaya Morskaya St., St. Petersburg, 191186, Russia

e-mail: KovLerEgo-student@ya.ru

**Abstract.** The issue is raised about the need to introduce a refresher course for employees of educational institutions in order to draw attention to the increasing cases of telephone fraud and the dissemination of information about techniques and measures to protect against fraud among students. It is becoming important to increase the financial and legal literacy of the population.

**Keywords:** professional development; fraud; cyber threats; social engineering; fraud schemes; anti-fraud measures; personnel training.

За последние годы случаи телефонного и интернет-мошенничества многократно увеличились. Под влияние мошенников попадают разные категории граждан [1]: от тех, кто не имеет образования, до тех, у кого есть высшее образование, людей с широким кругозором. Особенно много случаев с молодыми людьми, которые, помимо того, что становятся жертвами, еще могут быть вовлечены в преступную схему.

Несмотря на то, что каждый слышал о случаях мошенничества, опросы ВЦИОМ [2] фиксируют, что люди скептически относятся к тому, что могут быть обманутыми, однако практика показывает, что никто не застрахован.

Мошенники применяют методы социальной инженерии, разрабатывают многоходовые схемы, активно используют нейросети, фишинг, подмену номеров. По данным МВД, Центробанка и профильных аналитических



сервисов, таких как GetScam.com и Лаборатория Касперского, в 2024 году в России зафиксировано более 1,5 млн попыток телефонного мошенничества, что на 17 % больше, чем в 2023 году [3].

Фантазия мошенников безгранична, они придумывают новые схемы вовлечения граждан в «игру», переходя с одного этапа на последующие. Однако суть мошенничества остается такой же, как и была, есть разные признаки, по которым можно заподозрить обман.

Чаще всего используется запугивание — просят никому не сообщать, что звонят; «вежливые» угрозы и манипуляция — «это Ваши проблемы, мы хотим помочь», «Ваша семья может пострадать», «Сохраните деньги, Вы можете их лишиться»; просят продиктовать код (и он не обязательно от «Госуслуг»). Мошенники обманным путем получают доступ к «Госуслугам», даже если человек сам не сообщает им код из смс, и размещают там фальшивую доверенность на гражданина, преследуемого правоохранительными органами, используют различные чаты, аудио- и видеосвязь в мессенджерах, в том числе недавно появившихся.

Цель мошенников — деньги и то, что имеет ценность, поэтому неладное можно заподозрить, если звонившие просят перевести деньги на безопасный счет или задекларировать их. Поскольку бдительность граждан, в том числе благодаря СМИ и государству, растет, мошенники используют более сложные схемы, которые состоят из нескольких этапов [4–6]. Важно помнить, что различные ведомства не переключают друг на друга и звонят гражданам только чтобы пригласить их на встречу.

В связи с многократным привлечением молодых людей к административной и уголовной ответственности необходимо подготавливать сотрудников учебных заведений, повышать их квалификацию, чтобы в преподаваемые ими курсы включалась информация о защите от мошенников. Требуется четкое понимание и донесение до молодёжи различных схем, технических нюансов, которые применяют преступники — это значит, что необходимо повышать финансовую и правовую грамотность населения, как преподавателей, так и студентов.

#### СПИСОК ЛИТЕРАТУРЫ

1. Кибермошенничество: портрет пострадавшего // Банк России [Электронный ресурс]. URL: [https://cbr.ru/statistics/information\\_security/cyber\\_portrait/2024/](https://cbr.ru/statistics/information_security/cyber_portrait/2024/) (дата обращения: 15.09.2025).
2. ВЦИОМ. Новости: Телефонное мошенничество: мониторинг // ВЦИОМ [Электронный ресурс]. URL: <https://wciom.ru/analytical-reviews/analiticheskii-obzor/telefonnoe-moshennichestvo-monitoring?ysclid=mge7fr9iad892012490> (дата обращения: 15.09.2025).
3. Статистика телефонного мошенничества в РФ: тенденции и прогнозы. [Электронный ресурс]. URL: <https://abonentik.ru/blog/scam-stats-in-russia> (дата обращения: 15.09.2025).
4. Профилактика телефонного мошенничества // Официальный сайт МВД РФ [Электронный ресурс]. URL: <https://31.mvd.pf/citizens/pravo/pamyatki1/profilaktika-moshennichestva/profilaktika-telefonno-moshennichestva> (дата обращения: 15.09.2025).
5. Телефонное мошенничество: как противодействовать обману // Гарант.ру информационно-правовой портал. [Электронный ресурс]. URL: <https://www.garant.ru/article/1448451/?ysclid=mge7a3sqc8853389964> (дата обращения: 15.09.2025).
6. Телефонное мошенничество — виды и схемы обмана. Кибрарий – библиотека знаний по кибербезопасности. Всё самое важное и полезное о том, как защитить себя в цифровом мире // Сбербанк. (дата обращения: 15.09.2025).
7. Телефонные мошенники: какие схемы они используют для обмана // Аналитические статьи: ГАРАНТ.РУ. [Электронный ресурс]. URL: <https://www.garant.ru/article/1814213/?ysclid=mge9qkdjop899950558> (дата обращения: 15.09.2025).

УДК37.015.31

#### АВТОМАТИЗАЦИЯ БИЗНЕС-ПРОЦЕССОВ В СТУДИЯХ ЗВУКОЗАПИСИ: ВНЕДРЕНИЕ ЧАТ-БОТОВ И ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Мухин Максим Витальевич, Титова Розалия Андреевна

Российский государственный педагогический университет имени А. И. Герцена  
реки Мойки наб., 48, Санкт-Петербург, 191186, Россия  
e-mail: [titovaroza21@yandex.ru](mailto:titovaroza21@yandex.ru)

**Аннотация.** В статье рассматривается автоматизация бизнес-процессов в студиях звукозаписи с использованием современных информационных технологий, в частности, чат-ботов для оформления заказов и специализированного ПО для управления заказами. Подчеркивается важность безопасности информации при переходе от традиционных методов к более сложным системам.

**Ключевые слова:** программное обеспечение; чат-бот; Telegram; оформление заказа; управление информацией.

#### AUTOMATION OF BUSINESS PROCESSES IN RECORDING STUDIOS: CHATBOT IMPLEMENTATION AND INFORMATION SECURITY ISSUES

Mukhin Maxim, Titova Rosalia

Herzen State Pedagogical University of Russia  
48 Moika River Emb., St. Petersburg, 199406, Russia  
e-mail: [titovaroza21@yandex.ru](mailto:titovaroza21@yandex.ru)

**Abstract.** The article discusses the automation of business processes in recording studios using modern information technologies, in particular, chatbots for placing orders and specialized software for order management. The importance of information security is emphasized when moving from traditional methods to more complex systems.

**Keywords:** software; chatbot; Telegram; order placement; information management.

Развитие информационных технологий с каждым годом открывает всё больше возможностей для автоматизации любой работы. В сфере музыкальных услуг большим спросом пользуются студии записи и обработки звука, в которых теперь учёт бизнес-процессов происходит с помощью разного программного обеспечения (ПО), направленного на упрощение управления заказами студии.

Оформление заказов всё чаще происходит через взаимодействие с чат-ботами в социальных сетях и мессенджерах, таких как: ВКонтакте и Telegram.

Рассмотрим такое понятие, как чат-бот. Несмотря на повсеместное распространение чат-ботов в рамках digital-маркетинга и клиентского сервиса в целом, у данной технологии до сих пор не сформировалось единого и консолидированного определения. Данный концептуальный пробел во многом обусловлен различиями в методологических подходах к интерпретации ключевого для их функционирования понятия — «контекста».

Суть чат-бота в том, что это автоматизированный интерфейс, задача которого — провести пользователя от его запроса к результату с минимальными усилиями с обеих сторон. Он не просто «отвечает на вопросы», он совершает действия в определенной предметной области: бронирует, заказывает, консультирует, предоставляет доступ. Его ключевая ценность — в масштабируемости. Он позволяет автоматизировать рутинный, предсказуемый диалог, высвобождая человеческие ресурсы для решения по-настоящему сложных и творческих задач.

Современные системы диалогового взаимодействия принято классифицировать по уровню сложности их архитектуры. Выделяют два основных типа таких систем.

Первый тип — детерминированные (линейные) чат-боты. Их функционирование строится на жестко заданных алгоритмических сценариях и правилах. Диалог с пользователем происходит по предопределенному пути, часто с использованием кнопок или шаблонных ответов. Такие системы стабильны в работе, но обладают крайне ограниченной гибкостью и не способны обрабатывать запросы, выходящие за рамки заложенных в них инструкций.

Второй тип — интеллектуальные (недетерминированные) чат-боты, основанные на технологиях искусственного интеллекта и машинного обучения. Ключевой особенностью таких систем является способность к обучению и адаптации в процессе взаимодействия с пользователями. Благодаря использованию нейросетевых моделей они способны понимать контекст, распознавать интенции и обрабатывать мультимодальные данные — не только текст, но и изображения, аудио- и видеофайлы. Это позволяет им решать значительно более сложные задачи и обеспечивать более естественное взаимодействие (см. подробнее в работах [1-3]).

Таким образом, интеграция чат-бота в мессенджер Telegram предоставляет комплекс возможностей для оптимизации бизнес-процессов в студиях звукозаписи. В Telegram можно настроить ответ на популярные вопросы, выбор услуг при оформлении заказа, указание комментариев клиентом и прочие функции, которые заметно ускорят и упростят процесс оформления заказа. Чат-бота можно быстро и легко запрограммировать администратору системы, а для клиента это будет удобным вариантом потому, что такое оформление заказа не требует установки отдельных приложений, а предлагает связь со студией через привычный многим интерфейс Telegram.

Управление заказами и временем на студии с обычных Excel-таблиц всё чаще переходит в 1С, Битрикс, или вовсе в специально разработанные для конкретной студии продукты. С одной стороны, это приводит к ускорению и повышению эффективности работы студии, с другой — контроль за информацией теперь во многом относится к работе ПО. Если система спроектирована неверно, есть высокий шанс потери или утечки важной информации.

Рассмотрим пример информационной системы, в которой существуют следующие этапы управления информацией:

1. Оформление заказа клиентом через Telegram-бота.
2. Отправка информации о заказе на сервер с базой данных через API-сервер.
3. Запрос на информацию о заказе администратором через ПО для учёта заказов.
4. Чтение и управление информацией о заказе администратором через ПО для учёта.

В такой системе должно присутствовать регулярное резервное копирование. Информация проходит через множество облачных серверов, поэтому в ПО для учёта заказов важно предусмотреть функцию резервного копирования. Хранение информации на разных носителях может позволить восстановить базу данных при невозможности работы с сервером.

Тем не менее, хранение информации, например, на компьютере администратора студии является не до конца безопасным вариантом. Если другие люди получают доступ к компьютеру, они сразу получают доступ и к базе данных. Наличие проверки пароля при попытке подключения к базе данных может существенно обезопасить контроль и управление информацией. Если в студии работают несколько людей с разными должностями и с разным уровнем ответственности, можно предусмотреть идентификацию не просто ко всему функционалу ПО, а один уровень доступа для чтения и другой для чтения и редактирования.

Система должна быть спроектирована таким образом, чтобы клиент не мог получить доступ к информации о заказах других клиентов. Такое может произойти при неправильном проектировании чат-бота для оформления заказов, если присутствует функция показа заказов клиенту. Чат-бот должен строго ориентироваться на имя пользователя клиента при выводе информации, чтобы не показать информацию другого клиента. Можно предусмотреть установку и ввод пароля при попытке узнать информацию о заказе клиентом.

Так как оформление заказов и работа с ними касается персональных данных, помимо простых вводов паролей необходимо предусмотреть шифровку информации в базе данных, потому что всегда присутствует вероятность несанкционированного доступа от людей, которые захотят украсть персональные данные других людей. В Python существуют такие библиотеки, как `hashlib`, `PyCrypto`, `cryptography`, которые могут помочь зашифровать базу данных [4].

Наличие в системе алгоритмов шифрования данных и ввода паролей на каждом этапе работы с информацией может обезопасить как клиента, чью информацию не смогут узнать посторонние люди, так и администратора, на котором лежит основная ответственность за хранение всех данных в системе. При современных темпах развития информационных технологий важно помнить, что автоматизация информационных систем помимо комфорта и защиты данных от потери из-за человеческого фактора также приносит новые вопросы о безопасности, которые связаны с самим ПО, на что нельзя закрывать глаза.

В выпускной квалификационной работе «Разработка кроссплатформенных программных средств и мобильных сервисов поддержки проведения творческих мероприятий», которая была защищена в июне 2025 г. в стенах научно-методической лаборатории «Музыкально-компьютерные технологии» Российского государственного педагогического университета им. А. И. Герцена её автором — С.А. Жуковым была предложена схема решений ряда вопросов, обсуждаемых в данной статье [5]. Также в статьях коллег и партнёров по ведению совместных научно-исследовательских проектов, разрабатываемым на базе лаборатории [6; 7], рассматриваются вопросы, связанные с внедрением элементов теории нечётких множеств и систем искусственного интеллекта и обусловленные этим проблемы обеспечения информационной безопасности в процессе обработки и использования музыкального и — в целом — творческого контента.

Следовательно, инвестиции в безопасность ИТ-инфраструктуры, включая проектирование отказоустойчивых архитектур, внедрение протоколов шифрования и разработку регламентов управления доступом, являются критически важными и неотъемлемыми элементами современной системы управления студией. Игнорирование этих вопросов может привести к потерям, превышающим выгоды от внедрения самой автоматизации.

#### СПИСОК ЛИТЕРАТУРЫ

1. Слепцова Ю.Н. Автоматизация маркетинговых процессов при помощи чат-бота // Научный журнал. 2020. № 3 (48). URL: <https://cyberleninka.ru/article/n/avtomatizatsiya-marketingovykh-protsessov-pri-pomoschi-chat-bota> (дата обращения: 15.09.2025).
2. Романова Е.В., Двигубский А.В. Чат-боты как элемент управления системой // Хроноэкономика. 2019. № 7 (20). URL: <https://cyberleninka.ru/article/n/chat-boty-kak-element-upravleniya-sistemoi> (дата обращения: 15.09.2025).  
ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» // Официальный сайт электронного документа. [электронный ресурс]. URL: <https://itglobal.com/wp-content/uploads/2021/05/gost-57580.1-1.pdf> (дата обращения: 15.09.2025).
3. И. И. Иванов, А. А. Петров. Реализация криптографических методов защиты информации // Информация и безопасность : науч. журн. 2022. № 3. [электронный ресурс]. URL: [https://cchgeu.ru/science/nauchnye-izdaniya/nauchnyy-zhurnal-informatsiya-i-bezopasnost/texts\\_of\\_articles/2022/vypusk\\_3/%D0%98%D0%B8%D0%91%D0%B2%D1%8B%D0%BF%203%2022-2.pdf](https://cchgeu.ru/science/nauchnye-izdaniya/nauchnyy-zhurnal-informatsiya-i-bezopasnost/texts_of_articles/2022/vypusk_3/%D0%98%D0%B8%D0%91%D0%B2%D1%8B%D0%BF%203%2022-2.pdf) (дата обращения: 15.09.2025).
4. Жуков С.А. Разработка кроссплатформенных программных средств и мобильных сервисов поддержки проведения творческих мероприятий. Выпускная квалификационная работа. СПб., 2025.
5. Горбунова И.Б., Алиева И.Г. О проекте создания интеллектуальной системы по каталогизации и анализу музыки народов мира // Общество: философия, история, культура. 2016. № 9. С. 105-108.
6. Alieva I.G., Gorbunova I.B. A Transdisciplinary Approach to the Study of Musical Phenomena: Fuzzy Set Theory and Its Application to Music Research and Educational Practice. Russian Musicology. 2025. № 3, pp. 69–81.

УДК 004.8

#### ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ОБРАЗОВАНИИ: ПОДГОТОВКА КАДРОВ ДЛЯ ЦИФРОВОЙ ЭКОНОМИКИ

**Раковский Олег Владимирович, Аньшаков Артём Евгеньевич**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича  
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mails: rakovskii.ov@sut.ru, anshakov\_artem@mail.ru

**Аннотация.** Внедрение технологий искусственного интеллекта в образовании дает старт инновационным методам обучения. Повышается эффективность создания учебных материалов. Промежуточные тесты и экзамены генерируются в моменте. Появление нового цифрового сервиса, как биопротекторинг дает более субъективную и качественную оценку полученных знаний. Исключаются мошеннические действия при сдаче экзаменов и аттестаций. ИИ дает возможность разгрузить преподавательский состав. Профориентация, как глубокий анализ своих интересов и результатов через алгоритмы нейросети.

**Ключевые слова:** искусственный интеллект; образование; цифровая экономика; кадры.

#### ARTIFICIAL INTELLIGENCE IN EDUCATION: TRAINING FOR THE DIGITAL ECONOMY

**Rakovsky Oleg, Anshakov Artem**

The Bonch-Bruевич Saint Petersburg State University of Telecommunications,  
22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mails: rakovskii.ov@sut.ru, anshakov\_artem@mail.ru

**Abstract.** The introduction of artificial intelligence technologies in education gives rise to innovative teaching methods. The effectiveness of creating educational materials is improved. Intermediate tests and exams are generated at the moment. The emergence of a new digital service, such as bioprotection, provides a more subjective and qualitative assessment of the acquired knowledge. Fraudulent actions during exams and attestations are excluded. AI makes it possible to unload the teaching staff. Career guidance, as an in-depth analysis of your interests and results through neural network algorithms.

**Keywords:** artificial intelligence; education; digital economy; human resources.

В наше время с появлением ИИ стали возможны использование инновационных методов в обучении.

Появляются современные платформы для интерактивных курсов, онлайн сервисы, которые основаны на ИИ агентах [1]. ИИ может в помощь преподавателям проверять знания студентов, генерировать всевозможные задания и промежуточные тесты. Чат боты помогают студентам в ответе на интересующие вопросы и анализа полученных знаний.

Нейросети могут анализировать эмоциональное поведение студентов при прохождении экзаменов, аттестаций. Проверяют в режиме реального времени отвлечение взгляда от монитора, рабочего стола или другие нарушения при оценочных действиях. Такое решение получило название, как биопрокторинг — контроль прохождения теста по биометрическим параметрам (голос и изображение лица) [2].

ИИ агентов можно широко применять в индивидуальном обучении. На смену обычно репетиторству можно смело применять такие решения. ИИ сможет подсказать по иностранному языку или помочь с разбором решения задачи по высшей математике [3].

В работе выделены основные тезисы:

- ИИ применяется для совершенствования учебного процесса. Создание онлайн платформ обучения, интерактивных курсов. Все это способствует быстрому осваиванию и закреплению необходимых компетенций в максимально короткое время.

- ИИ вместо преподавателя. Нейросеть может полностью генерировать учебный процесс, отвечать на вопросы студентов, создавать промежуточные тесты, контрольные работы, субъективно оценивать результаты ответов, давать рекомендации к изучению.

- Рейтинги, ИИ трансформирует оценочную систему образования, центры оценок смещаются. Появление нового цифрового сервиса «Биопрокторинг». ИИ дает более объективную оценку качества учебного процесса и успеваемости студента.

- ИИ помощник в профориентации. Привычный тест на профотбор уходит в прошлое, в современное время нейросеть может на основе обучения и результатов поможет выявить определенные закономерности, еще до поступления в ВУЗ можно сориентироваться в выборе нужной профессии.

Подводя итог, можно отметить, что применение нейросетей в системе образования приносит массу плюсов. Рутинная, которой ранее были обременены преподаватели, перехватывают ИИ агенты. Формирование нового учебного плана можно сделать по определенным запросам и интересам, в том числе и персональный в добавок к основному. Оценка результатов знаний становится более субъективной и качественной.

#### СПИСОК ЛИТЕРАТУРЫ

1. Влияние ИИ на образование. [Электронный ресурс]. URL: <https://d-economy.ru/analitic/vlijanie-ii-na-obrazovanie/> (дата обращения: 28.08.2025). С. 18-19.
2. Биопрокторинг: студенты успешно протестировали новый сервис «Ростелекома» для дистанционной сдачи экзаменов. [Электронный ресурс]. URL: <https://www.kommersant.ru/doc/4947217> (дата обращения: 28.08.2025).
3. Курбанова З.С. Нейросети в контексте цифровизации образования и науки / З.С. Курбанова, Н.П. Исмаилова // Мир науки, культуры, образования. 2023. 3 (100). С. 309-311. DOI: 10.24412/1991-5497-2023-3100-309-311.

УДК 621.396.4

#### ОБУЧЕНИЕ И ПОВЫШЕНИЕ КВАЛИФИКАЦИИ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕГИОНАХ РОССИИ

**Ренсков Дмитрий Андреевич**

Военная академия связи им. Маршала Советского Союза С.М. Буденного,  
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия,  
e-mail: dmitryirenskov@gmail.com

**Аннотация.** В статье предлагаются меры по преодолению барьеров: создание региональных центров кибербезопасности, грантовые программы с обязательным трудоустройством, интеграция обучения с реальными задачами, развитие наставничества и сертификации. Подчеркивается, что только комплексная и долгосрочная стратегия, адаптированная к региональным особенностям, обеспечит устойчивый кадровый потенциал для технологического суверенитета и цифровой безопасности России.

**Ключевые слова:** информационная безопасность; кадры в сфере ИБ; обучение; повышение квалификации; регионы России; цифровая трансформация; кибербезопасность; профессиональные стандарты; онлайн-обучение; наставничество; импортозамещение.

## TRAINING AND PROFESSIONAL DEVELOPMENT INFORMATION SECURITY SPECIALISTS IN THE REGIONS OF RUSSIA

Renskov Dmitry

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny  
3 Tikhoretsky Av, St. Petersburg, 194064, Russia  
e-mail: dmitryirenskov@gmail.com

**Abstract.** The article suggests measures to overcome barriers: creation of regional centers cybersecurity, grant programs with compulsory employment, integration of training with real-world tasks, development of mentoring and certification. It is emphasized that only a comprehensive and long-term strategy adapted to regional specifics will ensure sustainable human resources for Russia's technological sovereignty and digital security.

**Keywords:** information security; personnel in the field of information security; training; advanced training; Russian regions; digital transformation; cybersecurity; professional standards; online training; mentoring; import substitution.

В условиях цифровизации и трансформации различных сфер информационная безопасность становится ключевой для национальной безопасности России. Особенно остро стоит проблема дефицита квалифицированных кадров в сфере кибербезопасности в регионах. Решение требует системного обучения и повышения квалификации с учетом региональных особенностей, и экономических возможностей.

1. Текущее состояние кадрового обеспечения в сфере информационной безопасности в регионах. По данным Минцифры России и аналитическим отчётам АНО «Цифровая экономика», дефицит специалистов по информационной безопасности в стране составляет более 60 тысяч человек, причём более 70% вакансий сосредоточено в регионах.

Основные причины кадрового дефицита: недостаточное количество профильных образовательных программ в региональных вузах и колледжах; отток молодых специалистов в крупные города (Москву, Санкт-Петербург, Екатеринбург, Новосибирск); низкий уровень заработной платы в государственных и муниципальных учреждениях по сравнению с коммерческим сектором; отсутствие системной мотивации для карьерного роста в сфере информационной безопасности на региональном уровне; недостаточная практическая направленность существующих программ обучения. Кроме того, многие действующие специалисты не проходят регулярное повышение квалификации.

2. Нормативно-правовая и институциональная база. Государство активно развивает нормативную базу, направленную на формирование кадрового потенциала в сфере информационной безопасности: Федеральный закон № 187-ФЗ «О безопасности КИИ» обязывает владельцев значимых объектов КИИ обеспечивать подготовку и аттестацию персонала; Национальная стратегия развития искусственного интеллекта, Стратегия цифровой трансформации регионов и дорожная карта «Кадры для цифровой экономики» ставят задачи по подготовке специалистов в области информационной безопасности; профессиональные стандарты (например, «Специалист по информационной безопасности», утверждённый Минтрудом) определяют требования к компетенциям.

На институциональном уровне функционируют: центры компетенций НТИ по направлению «Технологии кибербезопасности»; региональные центры цифровой трансформации, создаваемые при ведущих вузах; платформы непрерывного образования — «Сириус.Курсы», «Университет 2035», «Открытое образование»; Федеральные и региональные программы переподготовки — например, проекты Минцифры «Кадры для регионов», «Цифровые профессии».

Однако реализация этих инициатив в регионах сталкивается с рядом препятствий: отсутствием местных координаторов, слабой вовлечённостью работодателей, недостаточным финансированием и низкой информированностью потенциальных слушателей.

3. Современные форматы и технологии обучения.

Для решения проблемы нехватки кадров необходимо использовать гибкие, доступные и практико-ориентированные форматы обучения.

3.1. Онлайн-обучение и микрообучение.

Платформы дистанционного обучения позволяют специалистам из отдалённых регионов получать знания без отрыва от работы. Особое значение имеют: короткие модульные курсы (микрообучение) — позволяют освоить конкретные навыки (например, настройку SIEM, анализ логов); платформы MOOC — «Открытое образование», «Сириус.Курсы» — предлагают курсы по информационной безопасности, многие из которых бесплатны или субсидируются государством; геймификация и симуляторы — такие платформы, как Hack The Box, CyberPolygon, позволяют отрабатывать навыки в условиях, приближенных к реальным.

3.2. Практико-ориентированные программы.

Важно применять на практике: стажировки и лабораторные практикумы на базе региональных SOC, центров обработки данных, IT-компаний; кейс-метод и разбор реальных инцидентов — позволяет развивать навыки анализа и реагирования; участие в киберучениях — развивает командную работу и стрессоустойчивость.

3.3. Обучение на рабочем месте.

Для действующих сотрудников органов власти и государственных учреждений важно внедрять программы обучения в процессе работы. Менторство и наставничество — опытные специалисты передают знания новичкам. Ротация ролей — позволяет расширить кругозор и разобраться в смежных областях (например,

перейти от администрирования к анализу угроз). Внутренние киберполигоны — имитационные среды для отработки навыков без риска для реальных систем.

### 3.4. Корпоративные университеты и партнёрство с бизнесом.

Крупные IT-компании («Лаборатория Касперского», «Группа РСБ», «Ростелеком», «СберТех») развивают собственные образовательные программы и готовы сотрудничать с регионами: совместные академии и центры подготовки (например, «Академия Касперского», «Школа аналитиков ИБ Ростелекома»); программы стипендий и грантов для студентов и молодых специалистов; предоставление оборудования и лицензий для учебных лабораторий;

### 4. Региональные инициативы и передовой опыт.

Несмотря на общие проблемы, в ряде регионов уже реализуются успешные проекты по подготовке кадров в сфере информационной безопасности:

Татарстан: на базе Иннополиса создан Центр компетенций НТИ по кибербезопасности, который проводит обучение, стажировки для студентов и специалистов со всей России.

Свердловская область: запущена программа «КиберУрал», включающая обучение школьников, студентов и государственных служащих.

Ключевые элементы успеха: поддержка региональных властей — выделение бюджетов, создание нормативных стимулов; партнёрство с вузами и бизнесом — совместная разработка программ, стажировки, трудоустройство; акцент на практические навыки и трудоустройство — обучение ведётся с учётом конкретных вакансий и задач региона.

### 5. Проблемы и пути их решения.

Несмотря на наличие успешных кейсов, в большинстве регионов сохраняются серьёзные препятствия: финансовые ограничения — нехватка средств на обучение, оборудование, привлечение экспертов; организационная разобщённость — отсутствие единого координатора на региональном уровне; низкая мотивация сотрудников — отсутствие карьерных перспектив и материального стимулирования.

Предлагаемые меры:

1. Создание региональных центров кибербезопасности на базе ведущих вузов — как точек притяжения для обучения, исследований и трудоустройства.

2. Внедрение системы грантов и стипендий для студентов и специалистов, которые обязуются работать в регионе после окончания обучения.

3. Разработка региональных дорожных карт по кадрам в сфере информационной безопасности с чёткими KPI и ответственными исполнителями.

4. Интеграция обучения с реальными задачами — например, защита региональных порталов госуслуг или систем здравоохранения становится учебным проектом.

5. Развитие системы наставничества и сертификации — поощрение получения отраслевых сертификатов (CISSP, CEH, CompTIA Security+, отечественные аттестации ФСТЭК и ФСБ).

Для решения проблемы нужно комплексно совершенствовать образование, внедрять современные методы, привлекать бизнес и науку, а также создавать условия для специалистов. Только системный подход обеспечит безопасность и независимость России в цифровом мире.

## СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
2. Стратегия цифровой трансформации субъектов Российской Федерации (Минцифры РФ, 2023).
3. Дорожная карта «Кадры для цифровой экономики» (АНО «Цифровая экономика»).
4. Отчет «Дефицит кадров в сфере информационной безопасности: региональный разрез», РАНХиГС, 2024.
5. Материалы конференции «Киберобразование — 2024», Минобрнауки РФ.
6. Профессиональный стандарт «Специалист по информационной безопасности» (Приказ Минтруда №525н).
7. Практика регионов: кейсы Татарстана, Свердловской и Томской областей (официальные сайты правительств).

УДК 004.9

## ГЕЙМИФИКАЦИЯ УЧЕБНОГО ПРОЦЕССА В ИТ-УНИВЕРСИТЕТАХ: РИСКИ ПРИМЕНЕНИЯ

**Смородин Геннадий Николаевич, Файзуллин Радмир Ильдарович**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

Большевикова пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

e-mails: gsmorodin@gmail.com, renaos232@yandex.ru

**Аннотация.** Показано, что геймификация может быть стимулом повышения мотивации студентов и при ряде условий способствует внедрению командного подхода в учебный процесс факультетов информационных технологий и искусственного интеллекта. Показаны потенциальные риски дидактического и социально-психологического характера при применении элементов геймификации в учебном процессе. Рассмотрены мессенджеры как элементы геймификации. Отмечена спонтанность внедрения элементов геймификации.

**Ключевые слова:** геймификация учебного процесса; мотивация студенческого сообщества; спонтанность внедрения элементов геймификации; цифровая трансформация; софт скиллс.

## GAMIFICATION OF THE EDUCATIONAL PROCESS IN IT UNIVERSITIES: APPLICATION RISKS

Smorodin Gennadii, Faizullin Radmir

The Bonch-Bruевич Saint Petersburg State University of Telecommunications,  
22 Bolshhevikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mails: gsmorodin@gmail.com, renaos232@yandex.ru

**Abstract.** It is shown that gamification can be an incentive to increase students' motivation and, under a number of conditions, contributes to the introduction of a team approach into the educational process of the faculties of information technology and artificial intelligence. The potential risks of a didactic and socio-psychological nature in the application of gamification elements in the educational process are shown. Messengers are considered as elements of gamification. The spontaneity of the introduction of gamification elements is noted.

**Keywords:** gamification of the educational process; motivation of the student community; spontaneity of the introduction of gamification elements; digital transformation; soft skills.

В условиях цифровой трансформации образования геймификация (применение игровых элементов в целях повышения качества обучения) стала мощным инструментом для повышения мотивации, вовлеченности обучающихся и эффективности обучения студентов ИТ-специальностей [1,2].

Целью внедрения элементов геймификации является преодоление рутинности обучения, создание возможностей симуляции реальных профессиональных ситуаций развитие soft skills, применение командного подхода, формирование навыков решения задач в условиях ограниченного времени.

В целом применение геймификации в образовании носит сложный, противоречивый характер. Наряду с ускорением процесса обучения, с его «оживлением» и мотивацией к решению ситуационных задач, появляется риск «отстать от всех», потерять связь с развитием процесса обучения, основанного на игровых элементах [3].

Следует отметить, что использование интернет-мессенджеров (на данном этапе это в значительной степени Телеграм) также можно отнести к явлению геймификации. Студент одновременно в виртуальном мире участвует в нескольких текстовых беседах, возникающих часто спонтанно и требующих (или по крайней мере предполагающих) обратную связь в квази-реальном времени, в тоже время физически обучающийся находится, например, на аудиторных занятиях. Данное социальное явление еще ждет своей оценки исследователей, но возникающие здесь риски утраты эффекта от аудиторных занятий уже очевидны. Стремительное внедрение элементов искусственного интеллекта делает ситуацию еще менее предсказуемой. Фактически утрачивается грань между реальным и виртуальным аудио или текстовым собеседником. Для ИТ и ИИ направлений обучения применение геймификации — это не только способ организации учебного процесса, студенты непосредственно вовлечены в создание элементов геймификации. Значительная часть выпускных работ студентов бакалавриата и магистратуры связана с разработкой телеграм-ботов, игровых сервисов и мобильных приложений для профессиональной и социальной активности. И это говорит, что количество программных решений с элементами геймификации на рынке будет становится все больше и больше.

Таким образом, можно утверждать, что геймификация является перспективным, востребованным подходом для мотивации и обучения студентов, но ее применение во многом происходит спонтанно, без должной проработки и оценки перспектив, что порождает риск непредсказуемых последствий как социально-психологического, так и дидактического свойства.

### СПИСОК ЛИТЕРАТУРЫ

1. Ануфриева Ю.В. Геймификация как инструмент повышения мотивации обучающихся // МНКО. 2024. № 3 (106). URL: <https://cyberleninka.ru/article/n/geymifikatsiya-kak-instrument-povysheniya-motivatsii-obuchayuschisya> (дата обращения: 25.08.2025).
2. Гимельштейн Е.А., Годван Д.Ф., Стецкая Д.В. Применение инструментов геймификации в образовании // Бизнес-образование в экономике знаний. 2020. № 3 (17). URL: <https://cyberleninka.ru/article/n/primenenie-instrumentov-geymifikatsii-v-obrazovanii> (дата обращения: 25.08.2025).
3. Попова Т.В., Ермакова О.Е., Долгова А.А., Черных Н.А. Перспективы и риски внедрения геймификации в современном образовании // Вестник Костромского государственного университета. Серия: Педагогика. Психология. Социокинетика. 2022. № 2. URL: <https://cyberleninka.ru/article/n/perspektivy-i-riski-vnedreniya-geymifikatsii-v-sovremennom-obrazovanii> (дата обращения: 25.08.2025).



## МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА «ЭКОСИСТЕМА БЕЗОПАСНЫХ ГОРОДСКИХ ЦИФРОВЫХ СЕРВИСОВ»

УДК 004.9:351.9

### ЦИФРОВАЯ ИНКЛЮЗИЯ И КИБЕРБЕЗОПАСНОСТЬ ДЛЯ ЛЮДЕЙ С ОСОБЕННОСТЯМИ ЗДОРОВЬЯ И СОЦИОКУЛЬТУРНОЙ СРЕДЫ В РОССИИ

**Барандова Татьяна Леонидовна**

Северо-Западный институт управления - филиал РАНХиГС

Тучков пер., 7, Санкт-Петербург, 197101, Россия

e-mail: barandova-tl@ranepa.ru

**Аннотация.** Обозначены нормативные рамки и основные направления для работы государственных и общественных акторов по осуществлению цифровой инклюзии представителей социокультурных групп с особенностями здоровья и иных факторов, вызывающих проблемы в использовании цифровой среды сервисов социальной защиты. Процессы цифровой трансформации государственного управления, сформулированные в нормативных документах, затрагивают сферу социального обеспечения в условиях её реинжиниринга, обозначенного в указе «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» (май 2024 г.) в качестве приоритетов для формирования цифровой инфраструктуры. Комплексный анализ законодательства и практик реализации данного политического курса, показывает наличие «пробелов» в обеспечении инклюзивных проектов и кибербезопасности на практике, которые важно обозначить для усовершенствования механизмов осуществления недискриминационной цифровой трансформации в России.

**Ключевые слова:** цифровая инклюзия; цифровизация; цифровые трансформации; кибербезопасность; социальная политика.

### DIGITAL INCLUSION AND CYNERSECURITY FOR PEOPLE WITH HEALTH CONDITIONS AND SOCIOCULTURAL ENVIRONMENT IN RUSSIA

**Barandova Tatiana**

North-West Institute of Management - branch of RANEPa

7, Tuchkov Av, St. Petersburg, 197101, Russia

e-mail: barandova-tl@ranepa.ru

**Abstract.** The regulatory framework and main directions for the state's and public actors' activity in implementing digital inclusion of socio-cultural groups with health characteristics and other factors that cause problems in the use of the digital environment of social protection services are outlined. The processes of digital transformation of public administration are formulated in regulatory documents which affect the sphere of social security in the context of its reengineering, and outlined in the decree «On national development goals of the Russian Federation for the period up to 2030 and for the future until 2036» (May 2024) as priorities for formation of digital infrastructure. A comprehensive analysis of the legislation and practices for the implementation of this policy shows the presence of «gaps» in ensuring inclusive projects and cybersecurity in practice, which are important to identify in order to improve the mechanisms for implementing non-discriminatory digital transformation in Russia.

**Keywords:** digital inclusion; digitalization; digital transformations; cybersecurity; social policy.

Процессы цифровой трансформации в современном мире приобретают характер «тотализации» перехода всех акторов, являющихся реализаторами политических и управленческих функций государства, к технической опосредованности взаимодействий с обществом и гражданами. Сфера социальной политики, преимущественно в сегменте социального обеспечения и защиты населения, не является исключением. Приоритеты государственной политики в сфере цифровизации формируются с ориентиром на программные и нормативные документы, составляющие базовые основания, зафиксированные в ряде документов, включая: 1) положения Национального проекта «Экономика данных и цифровая трансформация государства» (30 марта 2024 г., Перечень поручений Президента по результатам послания Федеральному собранию); 2) целевые показатели и задачи, выполнение которых характеризует достижение цели «Цифровая трансформация государственного и муниципального управления, экономики и социальной сферы» (Указ Президента от 7 мая 2024 г. № 309);

Документы и показатели результативности, используемые в рамках деятельности по разработке стратегий цифровой трансформации отраслей экономики, социальной сферы, государственного управления субъекта Российской Федерации под руководством Минцифры России, внедряются в практическую работу



институций и организаций, осуществляющих поддержку социальных групп и категорий граждан, нуждающихся в предоставлении специальных мер социальной защиты, в т.ч. и тех, которые испытывают сложности в использовании цифровых экосистемных платформ и ИИ-продуктов и по причине состояния здоровья или в силу обстоятельств социокультурного характера (незнание русского языка, отсутствие доступа в интернет, цифровая неграмотность, потеря цифрового доверия ввиду перенесенных киберпреступлений, сверхконтроль со стороны внешних лиц, вкл. опеку, изоляция и блокировка доступа к сервисам, и т.п.). Относительно вопросов преодоления цифровой исключенности некоторых категорий граждан, уже предприняты шаги к разработке и внедрению специальных ИИ-продуктов на практическом уровне, в частности для людей с ограниченными возможностями по зрению и слуху используются программы, встраиваемые в девайсы, для осуществления коммуникации как в оффлайн, так и в онлайн среде, однако недостаточно учтены ситуативные факторы, касающиеся вопросов обеспечения им кибербезопасности. Нейрокомпьютерные интерфейсы для категорий лиц, которые лишены полностью обычных способов пользования ИКТ по состоянию здоровья, в частности, сюда попадают слепоглухонемые, люди с нарушением сенсорной моторики рук или их отсутствием, с глубокими ментальными расстройствами и т.п., в достаточно массовом производстве ещё не доступны. Особую озабоченность следует выразить и малоизученным эффектом «алгоритмической дискриминации», что в долгосрочной перспективе может привести к исключению больших сегментов населения, способных осуществлять нормальную жизнедеятельность в цифровой среде, но по разным причинам предпочитающих минимизировать соприкосновение с виртуализированными управленческими процессами (пока они доступны в реальной коммуникации). Спектр таких причин расширяется и ввиду продолжения сетцентрированного противостояния, которое переживает Россия, приводящего к нарушению моделей опосредованного цифровой средой общения с государственными и коммерческими инстанциями. Изучение их и выработка рекомендаций ещё предстоит.

Нормативные основы, регулирующие и введение цифрового управления в сферу социальной защиты, были сформированы в самом начале цифровой трансформации, либо до неё, поэтому нами проанализированы правовые положения следующих базовых направлений реализации социальной политики:

- Федеральный закон от 28.12.2013 № 442-ФЗ «Об основах социального обслуживания граждан в Российской Федерации», заложивший основу для создания электронных реестров поставщиков и получателей социальных услуг, позволяет подавать заявление на получение социальных услуг в электронной форме через портал Госуслуг, дистанционно заключать договоры на социальное обслуживание и формировать индивидуальную программу предоставления социальных услуг (ИППСУ) в цифровом виде. Вопросы обеспечения безопасности не отражены;

- Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» обеспечивает возможность для одиноких пожилых граждан подавать заявления на льготы, субсидии по ЖКУ и другие меры поддержки через портал Госуслуг без личного визита, используя механизм межведомственного электронного взаимодействия. Вопросы безопасности учтены минимально;

- Распоряжение Правительства РФ от 06.07.2021 № 1833-р «Об утверждении стратегии цифровой трансформации социальной сферы» — ключевой программный документ, задающий цели и сроки проектов (единые платформы, цифровые удостоверения, реестры и т.д.). Стратегия не содержит определений терминов, не отражает аспекты цифровой инклюзии категорий получателей социальной помощи, нет вопросов обеспечения кибербезопасности;

- Постановление Правительства РФ от 29.12.2023 № 2386 «О единой централизованной цифровой платформе в социальной сфере» — нормативный акт, регламентирует создание и функционирование цифровой платформы. Нет сведений о том, как она тестируется (проходит ли гражданскую экспертизу?) на практике использования.

Активно внедряются цифровые сервисы, включая создание единого информационного пространства и цифровых удостоверений для различных категорий граждан с целью унификации и оптимизации предоставления социальных услуг, что является положительным аспектом для молодых и здоровых групп населения, однако существуют и другие. Специализированное законодательство, регулирующее предотвращение алгоритмической и иных видов дискриминации разработаны слабо, но частично включены в правовую базу: а) Федеральный закон от 24.11.1995 № 181-ФЗ «О социальной защите инвалидов в Российской Федерации» основополагающий, все цифровые новации (ИПРА, платформа реабилитации, технические средства реабилитации) являются реализацией и развитием норм этого закона, но практика его реализации малоизучена; б) Федеральный закон от 29.12.2020 № 473-ФЗ (создает основу для создания и работы единого реестра и цифрового учета). К 2025 году планировался запуск единой централизованной цифровой платформы в сфере комплексной реабилитации инвалидов, что, возможно, улучшит взаимодействие с медико-социальной экспертизой и предприятиями по изготовлению средств реабилитации, включит искусственный интеллект и цифровой контроль в практику, но необходим общественный мониторинг её имплементации. С 1 марта 2025 года вступили в силу законы о социокультурной реабилитации инвалидов, учитывающие социальные нужды, включающие образовательные и трудовые аспекты, расширяющие понятие ИПРА, введена обязательная интеграция данных в Единую централизованную цифровую платформу (Постановлением Правительства РФ №2386 от 29.12.2023). Действует Программа «Социальный контракт» (в соответствии с Федеральным законом от 17.07.1999 № 178-ФЗ). В 2025 году расширены меры социальной поддержки ветеранов боевых действий, включая пенсионные выплаты, налоговые льготы, бесплатную медицинскую помощь и компенсации расходов

на жилье. Категория граждан, относящихся к инвалидам локальных конфликтов представляют особую группу (ФЗ от 12.01.1995 № 5 «О ветеранах»), перечень мер социальной поддержки и льгот, предоставляемых через цифровые сервисы с подтверждением электронными удостоверениями (одновременно социальной и банковской картой) и возможностью оформления дистанционно через личный кабинет и мобильное приложение. Необходим мониторинг практики, гражданская экспертиза нововведений, изучение «пробелов» кибербезопасности.

#### СПИСОК ЛИТЕРАТУРЫ

4. Боровков А.И., Незамаева О.Б., Болсуновская М.В., Елгина К.А., Алексей А.М., Бурлуцкая Ж.В. Поддержка принятия решений в социальной сфере на базе цифровой модели // Журнал исследований социальной политики. 2023. Т. 21, № 4. С. 677-692.
5. Талапина Э.В. Дискриминационный потенциал алгоритмов // Административное право и процесс. 2025. № 2. С. 55-58.
6. Фаллетти Э. Алгоритмическая дискриминация и защита неприкосновенности частной жизни // Journal of Digital Technologies and Law. 1 (2), 2023. С. 387-420.

УДК 321.7: 004.7

### ЦИФРОВОЕ ДОВЕРИЕ: ФАКТОРЫ УСТОЙЧИВОСТИ ВЗАИМОДЕЙСТВИЯ ГРАЖДАН И ВЛАСТИ ЧЕРЕЗ ЦИФРОВЫЕ ПЛАТФОРМЫ

Кутепова Дарья Олеговна

Университет ИТМО

Кронверкский пр., 49, Санкт-Петербург, 197101, Россия

e-mail: Kdo.Daria@yandex.ru

**Аннотация.** Цифровое доверие становится центральным элементом легитимности государственного управления в эпоху цифровой трансформации. В докладе представлен анализ факторов, обеспечивающих устойчивость взаимодействия между гражданами и органами власти через цифровые платформы. Исследование опирается на эмпирические данные международных индексов, экспертных интервью, опросов (2020–2024 гг.). Результаты исследования показывают, что устойчивость цифрового доверия определяется не столько технологической оснащённостью, сколько качеством институциональных отношений, прозрачностью процедур и степенью вовлечённости граждан. Особое внимание уделено роли цифровой грамотности, подотчётности власти и восприятия справедливости в формировании устойчивых цифровых практик взаимодействия.

**Ключевые слова:** цифровизация; цифровое доверие; общество и власть.

### DIGITAL TRUST: FACTORS OF SUSTAINABILITY OF INTERACTION BETWEEN CITIZENS AND AUTHORITIES THROUGH DIGITAL PLATFORMS

Kutepova Daria

University ITMO

49 Kronverksky Av, St. Petersburg, 197101, Russia

e-mail: Kdo.Daria@yandex.ru

**Abstract.** Digital trust is becoming a central element of the legitimacy of public administration in the era of digital transformation. The report provides an analysis of the factors ensuring the sustainability of interaction between citizens and authorities through digital platforms. The research is based on empirical data from international indices and expert interviews and surveys (2020-2024). It is shown that the stability of digital trust is determined not so much by technological equipment as by the quality of institutional relations, transparency of procedures and the degree of citizen involvement. Special attention is paid to the role of digital literacy, government accountability and the perception of justice in shaping sustainable digital interaction practices.

**Keywords:** digitalization; digital trust; society and government.

В настоящее время цифровое доверие является социально-политическим конструктом, отражающим готовность граждан взаимодействовать с государством через цифровые каналы на основе уверенности в надёжности, прозрачности и справедливости этих взаимодействий. Оно не сводится к технической безопасности, оно включает оценку институциональной легитимности и этичности цифровых процедур.

По результатам исследования стали известны ключевые факторы устойчивости цифрового взаимодействия:

- прозрачность алгоритмов и решений: граждане должны понимать, как и на каком основании принимаются решения (например, при назначении пособий или выдаче разрешений);
- подотчётность и обратная связь: наличие эффективных каналов для обращений, жалоб и предложений, а также демонстрируемая готовность власти реагировать на них;
- цифровая включённость и доступность: обеспечение равного доступа к цифровым сервисам для всех социальных групп, включая пожилых, маломобильных и жителей удалённых территорий [1];
- цифровая грамотность населения [2];
- безопасность персональных данных и невозможность утечки.

Институциональная легитимность выступает фундаментом цифрового доверия: даже самые многофункциональные платформы не смогут обеспечить устойчивое взаимодействие, если граждане не

воспринимают власть как легитимную и подотчётную. Стоит отметить, что автоматизация и ускорение государственных услуг сами по себе не ведут к росту доверия. При отсутствии прозрачности и механизмов участия цифровизация усиливает отчуждение и недоверие, особенно в случаях ошибок алгоритмов или отказов в услугах без возможности апелляции [3].

Отмечается, что устойчивость цифрового взаимодействия повышается, когда платформы не только предоставляют услуги, но и вовлекают граждан в процессы обсуждения, консультаций и совместного проектирования (например, через цифровые петиции, краудсорсинг нормотворчества, онлайн-слушания) [2].

Оперативное устранение неполадок и оперативное решения негативных ситуаций, а также интеграция механизмов участия и обратной связи в архитектуру всех государственных цифровых платформ может привести к повышению цифрового доверия в обществе.

#### СПИСОК ЛИТЕРАТУРЫ

1. ОЭСР. Индекс цифрового правительства: обеспечение цифровой трансформации государственного сектора. // Париж: Издательство ОЭСР, 2022. 124 с.
2. Горбач Л. А., Клименко Т. И., Зими́на И. В. Цифровое доверие как фактор цифровой трансформации экономической системы // Вестник Нижегородского университета им. Н. И. Лобачевского. Серия: Социальные науки. 2021. №3 (63) С. 19.
3. Мергель И. Определение цифровой трансформации: результаты экспертных интервью / И. Мергель, Н. Эдельманн, Н. Хауг // Government Information Quarterly. 2019. Т. 36, № 4. С. 1-16.

УДК 32.019.5

### АНАЛИЗ СОЦИАЛЬНОГО САМОЧУВСТВИЯ: КАК ЦЕНТР УПРАВЛЕНИЯ РЕГИОНОМ СТАНОВИТСЯ «СИГНАЛЬНОЙ СИСТЕМОЙ» ОБЩЕСТВЕННЫХ НАСТРОЕНИЙ

Негуляев Станислав Владимирович

Центр управления регионом  
Шпалерная ул. 51, Санкт-Петербург, 191015, Россия  
e-mail: st.negulyaev@gmail.com

**Аннотация.** Цифровизация публичного управления привела к созданию новых инструментов мониторинга общественных настроений. В условиях усиливающейся турбулентности (геополитической, экономической, технологической) социальное самочувствие становится фактором устойчивости регионального развития. В этом отношении наибольшую степень институционализации в России получили Центры управления регионом (ЦУР) — как аналитические центры и центры компетенций, функционирующие в цифровом информационном пространстве субъектов Российской Федерации. ЦУРы обладают функцией «цифровых рецепторов» — совокупности инструментов цифрового мониторинга и аналитики, способных в реальном времени считывать, агрегировать и интерпретировать сигналы общественных настроений: от прямых обращений и жалоб граждан до эмоциональной окраски открытых дискуссий в социальных сетях. Возможность ЦУР отслеживать общественные настроения в реальном времени предоставляет властям эффективный инструмент для оперативного выявления точек социального напряжения, принятия превентивных управленческих решений и, как следствие, поддержания доверия граждан — ключевого ресурса устойчивого развития регионов.

**Ключевые слова:** мониторинг; обратная связь граждан; публичное управление; цифровизация; Центр управления регионом.

### SOCIAL WELL-BEING ANALYSIS: HOW THE REGIONAL MANAGEMENT CENTER BECOMES A «SIGNAL SYSTEM» OF PUBLIC OPINION

Negulyaev Stanislav

Regional Management Center  
51 Shpalernaya St., St. Petersburg, 191015, Russia  
e-mail: st.negulyaev@gmail.com

**Abstract.** The digital transformation of public administration has led to the emergence of new tools for monitoring public sentiment. In the context of growing turbulence—geopolitical, economic, and technological—social well-being has become a critical factor for the sustainable development of regions. In this regard, Regional Management Centers (RMCs) have achieved the highest degree of institutionalization in Russia, functioning as analytical hubs and centers of competence within the digital information space of the Russian Federation's constituent entities. RMCs operate as “digital receptors”—a suite of digital monitoring and analytics tools capable of reading, aggregating, and interpreting signals of public sentiment in real time, ranging from citizens' direct appeals and complaints to the emotional tone of open discussions on social media. This real-time capacity to track public sentiment provides authorities with an effective instrument for promptly identifying hotspots of social tension, implementing preventive management decisions, and, consequently, maintaining public trust — a key resource for regional sustainable development.

**Keywords:** monitoring; citizen feedback; public administration; digitalization; Regional Management Center.

Глобальные политические сдвиги и ускорение процессов цифровой трансформации подталкивают государство к созданию более современных форм общественного взаимодействия, включая цифровые платформы и социальные медиа. Руководители государственных организаций всё больше сталкиваются

с возрастающими требованиями к открытости внутренних процессов, предоставления полной и качественной информации о деятельности государственных органов и организаций. Обратной стороной этого процесса является трансформация природы угроз в информационной сфере: неконтролируемое тиражирование «фейков» и дезинформация, использование технологий «социальной инженерии», целенаправленная компрометация государственных институтов, «бумажные атаки» — организованное давление через массовые обращения и жалобы, и многое другое.

Классические модели информационного противостояния дополнились новыми стратегиями воздействия, которые в научной литературе определяются через понятие «когнитивные войны» [1].

Такая ситуация грозит не только выведением из доверия институтов государственной власти, но и ставят под угрозу устойчивость управления на региональном уровне. Ответом на это стал процесс подъёма институтов мониторинга социального состояния общества [2]. Институциональное оформление процесса мониторинга общественных настроений и обратной связи в России произошло через создание в 2020 году и дальнейшее масштабирование модели Центров управления регионом (ЦУР) на все субъекты Российской Федерации, включая новые территории.

Для этого в каждом регионе сформирован комплекс цифровых инструментов, позволяющий объединить обратную связь, социальные медиа и аналитические данные в единую систему управленческой поддержки.

В настоящее время ЦУР осуществляет системную работу с пятью ключевыми информационными системами мониторинга и обратной связи:

1. Платформа обратной связи «Госуслуги. Решаем вместе». Платформа создана в рамках федерального проекта «Цифровое государственное управление» и стратегического национального проекта «Цифровая экономика». Обеспечивает приём и сопровождение обращений граждан с возможностью оперативного контроля за ходом их решения. Включает специализированный модуль для проведения онлайн-опросов, общественных обсуждений, голосований и слушаний по социально значимым вопросам, что предоставляет гражданам возможность реализовать своё право на авторизованное участие в принятии решений при реализации государственных и общественных инициатив.

2. Система мониторинга социальных медиа «Инцидент-менеджмент». Позволяет отслеживать открытые публикации в социальных сетях, выявлять информационные поводы, сигналы общественного недовольства и оперативно публиковать официальные ответы от имени исполнительных и местных органов власти, обеспечивая прозрачность и своевременность обратной связи. Поиск сообщений производится, по ключевым словам, и сочетаниям, чаще всего относящихся к социальным вопросам. Результаты мониторинга поступают к региональному администратору, который решает, какие «инциденты» нуждаются в реакции властей. Выбранные сообщения сортируются по профилям на уровне местного самоуправления или отраслевых органов в зависимости от принадлежности полномочий [3].

3. Информационно-аналитическая система «Призма». Предназначена для повышения эффективности регионального управления за счёт применения современных технологий поддержки принятия решений. Обеспечивает информационно-аналитическую поддержку субъектов Российской Федерации, органов государственной власти, органов местного самоуправления в сфере социально-экономического и общественно-политического развития, а также обеспечения комплексной безопасности. Система обеспечивает мониторинг ключевых показателей деятельности органов исполнительной власти субъектов Российской Федерации и формирует аналитическую основу для стратегического планирования и оценки результативности управленческих решений [4].

4. Система «Госпаблики». Обеспечивает централизованное управление сетью региональных госпабликов, объединяя их в единую платформу для координации информационных потоков и реализации согласованной коммуникационной стратегии. На сегодняшний день официальные страницы органов государственной власти являются не только средством для получения важной информации о деятельности государственных организаций, но и пространством для цифровых политических коммуникаций с гражданами. Центры управления регионом назначены ответственными за методическое сопровождение, развитие и координацию деятельности «госпабликов» на территории каждого субъекта Российской Федерации.

5. Тепловая карта ЦУР. Представляет собой инструмент агрегирования и визуализации данных, поступающих из платформы обратной связи «Госуслуги. Решаем вместе» и системы мониторинга социальных медиа «Инцидент-менеджмент». Карта отображает территориальные точки социального напряжения и наиболее частые запросы населения на основе территориальной привязки. Тепловая карта ЦУР позволяет оперативно выявлять «горячие» зоны, анализировать причины возникновения проблем и разрабатывать превентивные управленческие меры для их устранения.

Институциональное устройство ЦУР формирует основу для нового типа управленческой практики, ориентированной на постоянное считывание и интерпретацию «сигналов» социального самочувствия граждан. При помощи функций «цифровых рецептов» (интегрированных информационных систем) ЦУР способен в реальном времени выявлять точки напряжения и оперативно реагировать на запросы граждан.

Таким образом, Центры управления регионом (ЦУР) выступают важным элементом цифровой трансформации публичного управления в России, обеспечивая институционализацию мониторинга и анализа общественных настроений. Деятельность ЦУР способствует выработке обоснованных управленческих решений, повышению устойчивости региональных органов власти и укреплению доверия граждан к государственным институтам.

Перспективы модели работы ЦУР связаны с переходом от оперативного реагирования к стратегической аналитике, направленной на выработку системных решений и повышение устойчивости регионального развития.

#### СПИСОК ЛИТЕРАТУРЫ

1. Медушевский А.Н. Когнитивная война: социальный контроль, управление сознанием и инструмент глобального доминирования (часть 1) // Вопросы теории и практики управления. 2023. № 2. С. 88.
2. Mulgan, R. G. Making open government work. New York, NY: Palgrave-Macmillan, 2014.
3. Панфилов, И.А., Гришин, З.И., Митрофанова, Д.В. Проектирование систем Инцидент-менеджмента для регионального управления / И.А. Панфилов, З.И. Гришин, Д.В. Митрофанова // Решетневские чтения, материалы науч.-практ. конф. Красноярск. 2021. С. 345-347.
4. Ведомости // «Призма» — готовое решение для анализа показателей регионов URL: [https://www.vedomosti.ru/press\\_releases/2019/04/30/prizma--gotovoe-reshenie-dlya-analiza-pokazatelei-regionov](https://www.vedomosti.ru/press_releases/2019/04/30/prizma--gotovoe-reshenie-dlya-analiza-pokazatelei-regionov) (дата обращения: 14.09.2025).

УДК 004.9:351.9

### ВОСПРИЯТИЕ БЕЗОПАСНОСТИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ С ИИ В КОММЕНТАРИЯХ ПОЛЬЗОВАТЕЛЕЙ

Низомутдинов Борис Абдуллохонович

Университет ИТМО

Кронверкский пр., 49, Санкт-Петербург, 197101, Россия

e-mail: boris@itmo.ru

**Аннотация.** В исследовании анализируется пользовательское восприятие безопасности мобильных приложений с искусственным интеллектом на основе более 10000 отзывов из маркетплейса. Результаты показывают, что менее 3% отзывов непосредственно затрагивают вопросы безопасности. Среди выявленных проблем преобладают три ключевых направления: непрозрачность платежей и подписок, конфиденциальность и обработка персональных данных, а также общая безопасность информации. Значительно реже пользователи выражают обеспокоенность трансграничной передачей данных и проблемами доступа к аккаунтам. Проблемы безопасности концентрируются в наиболее критичных для доверия пользователей областях. Исследование демонстрирует, что повышение прозрачности финансовых условий, политик обработки данных и предсказуемости модерации является ключевым фактором для укрепления пользовательской лояльности и ответственного внедрения ИИ-технологий.

**Ключевые слова:** мобильные приложения; ИИ; отзывы; безопасность; комментарии; парсинг.

### THE PERCEPTION OF THE SECURITY OF MOBILE APPLICATIONS WITH AI IN USER COMMENTS

Nizomutdinov Boris

ITMO University

49, Kronverksky Av, St. Petersburg, 197101, Russia

e-mail: boris@itmo.ru

**Abstract.** The study analyzes the user's perception of the security of mobile applications with artificial intelligence based on more than 10000 reviews from the marketplace. The results show that less than 3% of the reviews directly address safety issues. Three key areas prevail among the identified problems: non-transparency of payments and subscriptions, confidentiality and processing of personal data, as well as general information security. Users are much less likely to express concern about cross-border data transfer and account access issues. Security issues are concentrated in the most critical areas for user trust. The study demonstrates that increasing transparency of financial conditions, data processing policies, and predictability of moderation is a key factor for strengthening user loyalty and responsible implementation of AI technologies.

**Keywords:** mobile app; AI; reviews; security; comments; parsing.

В последние годы технологии искусственного интеллекта (ИИ) активно внедряются в мобильные приложения. Расширение областей применения повышает требования к надёжности и безопасности ИИ, включая устойчивость к атакам, защиту конфиденциальности и управляемость моделей. Масштабирование ИИ обостряет уязвимости на уровне алгоритмов и инфраструктуры. В медицине внедрение ИИ улучшает скорость диагностики, создавая предпосылки для «высокоэффективной медицины» [1]. Однако критическое значение имеют качество данных, прозрачность решений и надёжность алгоритмов, что определяет требования к безопасности и доверию. Фундаментальные риски связаны с враждебными атаками на модели. Исследования демонстрируют, что целенаправленные длительные воздействия на модели могут нарушать работу систем в критичных областях [2]. Для мобильных приложений это также создаёт риски эксплуатации. Отдельную проблему представляют утечки данных через поведение модели. Атаки при запросах позволяют установить, использовались ли конкретные записи при обучении, даже без доступа к параметрам модели, исследования показывают, как даже защищенные системы позволяют извлекать личную информацию, приводя к утечкам в сеть. [3].

Таким образом, устойчивость к атакам и защита конфиденциальности остаются ключевыми условиями ответственного внедрения ИИ. Современные исследования подтверждают необходимость соблюдения

принципов безопасности, аудита моделей и прозрачности жизненного цикла данных, особенно в пользовательских и мобильных сценариях.

В контексте мобильных приложений с ИИ особое значение приобретает субъективное восприятие безопасности пользователями. Для изучения этого аспекта в данной работе предлагается анализировать пользовательские отзывы о мобильных приложениях с ИИ. Методология включает выявление сообщений, связанных с темами безопасности, их последующую классификацию и содержательный анализ. Такой подход позволяет выявить не только реальные уязвимости, но и субъективные тревоги пользователей, формирующие барьеры для внедрения технологий.

Первоначальный план исследования предусматривал сбор данных из магазина приложений Google Play. Однако в 2025 году доступ к данному ресурсу ограничен у ряда интернет-провайдеров. В связи с этим принято решение использовать в качестве источника данных российский маркетплейс RuStore. Данный выбор оказался верным, поскольку платформа демонстрирует растущую популярность и в большей степени отражает актуальный пользовательский опыт, по сравнению с Google Play.

Методология исследования включала несколько последовательных этапов. На первом этапе с помощью встроенной функции поиска маркетплейса были найдены приложения, в описании которых присутствовали упоминания технологий искусственного интеллекта. Далее с помощью специально разработанного парсера была выгружена информация с маркетплейса в базу данных, содержащая перечень приложений, их описания и пользовательские оценки по шкале от 0 до 5. Из этого списка были отобраны наиболее популярные приложения, для которых был осуществлен сбор текстовых отзывов. Ввиду отсутствия публичного API RuStore, сбор отзывов также проводился с применением парсинга. На заключительном этапе проведена классификация собранных отзывов: были выделены сообщения, связанные с проблематикой безопасности, которые в дальнейшем были разделены по тематическим категориям для проведения итогового анализа пользовательского восприятия.

Всего выявлено 385 приложений, из которых подавляющее большинство напрямую заявляет об интеграции ИИ в своём функционале. Незначительное количество позиций не имеют явных указаний на использование ИИ в описании и, вероятно, включены в выборку при поиске ошибочно. Для структурирования данных приложения были классифицированы по основным тематическим группам. Наибольшую долю в 35%, составляют «Чат-боты и виртуальные ассистенты». Группа «Генерация и редактирование изображений и видео» занимает около 20%. Приложения для «Общения с ИИ-персонажами и виртуальными партнёрами» составляют 10%. Остальные категории распределили между собой оставшиеся 35%. Наивысшие оценки (около 4.5-4.8) демонстрируют приложения из групп «Виртуальные собеседники» и «Генерация изображений», тогда как универсальные «Чат-боты» имеют средний балл около 3.0, что может указывать на завышенные ожидания пользователей или несовершенство реализаций.

На следующем этапе были отобраны наиболее популярные приложения, собраны отзывы и выделены сообщения по теме безопасности. Тексты отзывов приведены к единому виду, упоминания безопасности выявлены гибридным способом — по словарю характерных маркеров и по результатам обученной классификационной модели. Близкие по смыслу сообщения сгруппированы для выделения подтем. Проведенный анализ более 10000 отзывов о мобильных приложениях на основе ИИ показал, что тема безопасности волнует пользователей, но не является доминирующей. Менее 3% всех отзывов затрагивают безопасность. Внутри этой доли ключевыми остаются три направления: платежи и подписки (~45%), где пользователей тревожат непрозрачные условия, сложности с отменой автопродления, двойные списания и медленная поддержка; конфиденциальность и обработка данных (~30%), включая вопросы о месте и способах хранения, доступе разработчиков к перепискам и отсутствие локализованных политик; а также сохранности информации и защита детей (~15%), несостыковки между заявленными ограничениями и фактической модерацией, отсутствие возрастной верификации. Дополнительно отмечаются опасения по трансграничной передаче данных и юрисдикции (~7%), а также эпизодические претензии к требуемым интеграциям (~2%) и проблемам с аккаунтом и доступом (~1%).

Тема безопасности не доминирует количественно, но концентрируется в областях, критичных для доверия; устранение рисков в платежной прозрачности, конфиденциальности и предсказуемости модерации наиболее повысит лояльность и удовлетворенность. В целом, низкий процент отзывов о безопасности может означать, что большинство пользователей либо доверяют приложениям, либо не задумываются о рисках, что также несет в себе угрозу. Тем не менее, разработчикам стоит уделять внимание этим аспектам. Усиление прозрачности в отношении использования данных и явное согласие на установку могут значительно повысить уровень доверия.

Проведенный анализ пользовательских отзывов выявил критически важную закономерность: низкий процент упоминаний проблем безопасности, составляющий менее 3%, свидетельствует не об отсутствии рисков, а о недостаточной осведомлённости и рефлексии пользователей о потенциальных угрозах, связанных с использованием ИИ-приложений. Данный факт представляет собой скрытую системную уязвимость всей экосистемы. Мобильные приложения с искусственным интеллектом объективно несут комплексные угрозы, включая риски несанкционированного сбора и утечки персональных данных, манипуляции пользовательским поведением через персонализированные алгоритмы, а также финансовые потери. Низкий уровень обеспокоенности со стороны конечных пользователей не только усугубляет эти риски, создавая иллюзию безопасности, но и сигнализирует о необходимости безотлагательных превентивных мер. В связи с этим вопросам безопасности необходимо уделять повышенное и системное внимание на всех уровнях управления цифровой средой. Это требует скоординированных действий как со стороны площадок-распространителей,

которые должны ужесточить проверки и требования к разработчикам, особенно в части прозрачности политик конфиденциальности и механизмов подписок, так и со стороны регуляторов, и установление четкой ответственности за нарушения. Только такой комплексный подход позволит минимизировать потенциальный ущерб и обеспечить безопасное и устойчивое развитие технологий искусственного интеллекта в мобильной экосистеме в долгосрочной перспективе.

*Исследование выполнено при финансовой поддержке гранта Российского научного фонда № 25-28-00217, <https://rscf.ru/project/25-28-00217/> «Дифференциация практик использования технологий искусственного интеллекта в среде жителей мегаполиса: социологический анализ».*

#### СПИСОК ЛИТЕРАТУРЫ

1. Topol E. J. High-performance medicine: the convergence of human and artificial intelligence / E. J. Topol // Nature Medicine. 2019. Vol. 25, № 1. P. 44–56. DOI: 10.1038/s41591-018-0300-7.
2. Biggio B. Wild patterns: Ten years after the rise of adversarial machine learning / B. Biggio, F. Roli // Pattern Recognition. 2018. Vol. 84. P. 317–331. DOI: 10.1016/j.patcog.2018.07.023.
3. Practical Secure Aggregation for Privacy-Preserving Machine Learning / K. Bonawitz, V. Ivanov, B. Kreuter [et al.] // Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17). New York, NY, USA : Association for Computing Machinery, 2017. P. 1175–1191. DOI: 10.1145/3133956.3133982.

УДК 004.9:351.9

### ИСПОЛЬЗОВАНИЕ МЕТОДА ВКЛЮЧЁННОГО НАБЛЮДЕНИЯ ПРИ ИЗУЧЕНИИ СЕРВИСОВ ЭЛЕКТРОННОГО УЧАСТИЯ: ПЕРСПЕКТИВЫ И ОГРАНИЧЕНИЯ

Панфилов Георгий Олегович<sup>1</sup>, Коваленко Наталия Николаевна<sup>2</sup>

<sup>1</sup> Университет ИТМО,

Кронверкский пр., 49, Санкт-Петербург, 197101, Россия,

<sup>2</sup> Санкт-Петербургский государственный аграрный университет,

Петербургское ш., 2, Санкт-Петербург, 1196601, Россия,

e-mails: panfilovgeorg@mail.ru; turdusmerulan@yandex.ru

**Аннотация.** В тезисах представлены результаты попытки применения метода включенного наблюдения (Participant observation) для исследования результативности сервисов электронного гражданского участия в России. Авторами было проведено два пилотных исследования, в рамках которых были направлены 58 и 136 электронных обращений по реальным общественным проблемам. Был произведен сравнительный анализ полученных результатов и сделаны выводы о перспективах и ограничениях применения метода для исследования сервисов электронного участия.

**Ключевые слова:** метод включенного наблюдения; электронное участие; электронные обращения.

### APPLICATION OF THE PARTICIPANT OBSERVATION METHOD IN THE STUDY OF E- PARTICIPATION SERVICES: PROSPECTS AND LIMITATIONS

Panfilov Georgiy<sup>1</sup>, Kovalenko Natalia<sup>2</sup>

<sup>1</sup> ITMO University,

49 Kronverksky Ave., 197101 Saint Petersburg, Russia,

<sup>2</sup> Saint-Petersburg State Agrarian University,

2 Petersburg highway, 196601 Saint Petersburg, Russia,

e-mails: panfilovgeorg@mail.ru; turdusmerulan@yandex.ru

**Abstract.** This paper presents the results of an attempt to use participant observation to study the effectiveness of e-participation services in Russia. To this end, the authors conducted two pilot studies, in which 58 and 136 e-appeals were sent on real social issues. A comparative analysis of the results was conducted, and conclusions were drawn regarding the prospects and limitations of this method for studying e-participation services.

**Keywords:** participant observation; e-participation; e-appeals.

Одним из ключевых явлений, находящихся в поле зрения исследователей цифровизации государственной политики и управления, является электронное участие граждан [1]. Явление исследуется представителями как общественных наук – политологии, социологии, юриспруденции, государственного и муниципального управления, так и технических наук, прежде всего прикладных направлений информатики [2]. На сегодняшний день можно выделить два основных подхода к прикладным исследованиям электронного участия, в том числе применяемых в российских исследованиях. Первый подход условно можно обозначить как изучение электронного участия с точки зрения предложения, второй – как изучение с точки зрения спроса. В первом случае исследовательский вопрос фокусируется на том, что представляют собой сервисы электронного участия, «предлагаемые» государством гражданам. Во втором случае исследовательский вопрос касается особенностей «спроса» граждан на предлагаемый им «продукт» (их востребованность у граждан, удовлетворенность и т.д.). В случае изучения участия с точки зрения спроса наиболее частые методы исследований – это опросы и анкетирования граждан, мониторинг показателей активности на электронных ресурсах (например, данные о

количестве пользователей, поданных обращений и т.д.). В случае изучения с точки зрения предложения основные методы это мониторинг и бенчмаркинг функциональных возможностей электронных ресурсов.

При этом перечисленные методы обладают существенным недостатком: они фокусируют свое внимание скорее на внешних сторонах электронного участия, не уделяя должного внимания фактической результативности работы сервисов, достижения гражданами и органами власти конструктивного согласия при взаимодействии. Данного недостатка во многом лишен метод контент-анализа результатов электронного участия (тексты обращений и т.п.), позволяющий оценить, привели ли они к желаемому результату [3]. Также недостаток информации о фактической результативности сервисов электронного участия, позволяет достичь использование метода экспертных интервью с представителями ключевых акторов процесса электронного участия (органы государственной власти, гражданские активисты, компании-разработчики), обладающих экспертными знаниями о преимуществах и недостатках используемых сервисов [4]. При этом в ряде случаев информация о работе сервисов является закрытой, что накладывает ограничения на использование указанных методов.

Для решения проблемы недостатка информации о фактической результативности сервисов электронного участия авторами был поставлен вопрос о перспективности применения метода включенного наблюдения для сбора данных. Метод включенного наблюдения (Participant observation) – качественный метод исследования, предполагающий, что исследователь сам становится участником изучаемого процесса и производит наблюдения в полевых условиях. Наиболее широкое применение метод нашел в социально-антропологических исследованиях и использовался для изучения социальных отношений в традиционных и менее развитых обществах [5]. В социально-политических исследованиях метод начал использоваться с 1960-70-ых гг. для изучения поведения государственных служащих [6]. В современных российских исследованиях метод также продолжает использоваться при изучении особенностей работы органов государственной власти и местного самоуправления [7]. Отдельные исследования посвящены аспекту взаимодействия органов государственной власти с гражданами, открытости органов власти при предоставлении информации о своей деятельности [8].

Для оценки перспективности и целесообразности использования метода включенного наблюдения для исследования сервисов электронного гражданского участия авторами была разработана методика и произведены пилотные исследования по следующему принципу. В качестве канала участия были выбраны электронные обращения граждан, направляемые через такие каналы как электронная приемная, Платформа обратной связи портала государственных и муниципальных услуг (ПОС ЕПГУ) и региональный портал Наш «Санкт-Петербург» как каналы, работа которых регулируется нормативно-правовыми актами разного уровня. Была произведена регистрация на данных электронных ресурсах и направлены обращения по реально-существующим общественным проблемам в ответственные органы государственной власти. На обращения были получены ответы, была оценена реакция ответственных органов власти на описанные проблемы. Первое пилотное исследование включило в себя 58 обращений по обращениям разных категорий (благоустройство, экология, ремонт дорог, социальная сфера и др.) [9]. Второй этап исследования включил в себя написание 136 обращений в двух субъектах РФ – Санкт-Петербурге и Ленинградской области по одной проблеме – зарастание территорий борщевиком Сосновского [10]. Применение метода включенного наблюдения позволило собрать данные о сроках ответа и реагировании ответственных органов государственной власти или местного самоуправления на заявленные проблемы и классифицировать их по следующему принципу: (1) Проблема полностью решена, (2) проблема полностью решена после повторных/повторного обращений, (3) проблема частично решена, (4) проблема частично решена после повторных/повторного обращений, (5) предоставлен промежуточный ответ (решение проблемы запланировано на более поздний срок, (6) предоставлен бессодержательный формализованный ответ (отписка), (7) предоставлен отказ в решении проблемы.

Собранные при использовании метода включенного наблюдения данные позволили произвести сравнительный анализ результативности решения общественных проблем и скорости ответов по следующим критериям: (1) Канал электронного участия (электронная приемная, ПОС, «Наш Санкт-Петербург»), (2) временной критерий (с 2021 по 2025 год), (3) территориальный критерий (субъект РФ, административный район), (4) категория обращения (благоустройство, дороги, социальная сфера и т.д.), (5) объект (парк / газон на улице / загородная территория и т.д.), (6) ответственный исполнитель (Комитет / Администрация района/ подведомственное учреждение и т.д.) Проведенный сравнительный анализ позволил осуществить проверку ряда гипотез о влиянии отдельных факторов на результативность решения проблем, о которых было сообщено гражданами в электронных обращениях. В том числе были проверены гипотезы о влиянии на результативность решения проблем таких факторов как степень проработанности регионального законодательства (не подтвердилась), уровень урбанизированности территории (подтвердилась) и некоторых других.

Метод включенного наблюдения показал свою результативность для исследования сервисов электронного гражданского участия, позволил собрать качественные данные и частично восполнить недостаток знаний о фактической результативности сервисов электронного участия и особенностей коммуникации граждан и органов власти по общественным проблемам в электронной форме. В качестве ключевых преимуществ применения метода стоит отметить возможность исследователя изучить процесс изнутри от лица пользователя-гражданина, а также возможность верификации собранных данных (возможность проверки решения проблем и написания повторных обращений). В качестве недостатка применения метода следует его высокую затратность в части временных ресурсов, сложность сбора большой выборки, и, как следствие, возможную проблему репрезентативности данных. Исследование будет продолжено авторами, сбор данных с использованием метода включенного наблюдения будет масштабирован на другие территории, сервисы и тематики обращений.



## СПИСОК ЛИТЕРАТУРЫ

1. Чугунов А. В. Электронное участие в контексте трансформации концепции демократии // Управленческое консультирование. 2017. № 8. С. 14-20. <https://doi.org/10.22394/1726-1139-2017-8-14-20>.
2. Sæbø Ø., Rose J., Flak L.S. The shape of eParticipation. Characterizing an emerging research area // Government Information Quarterly. 2008. Vol. 25 (3). P. 400-428.
3. Быков И. А. Цифровые платформы государственного управления в системе национальных публичных коммуникаций // Журнал политических исследований. 2021. № 2. С. 45-56. <http://doi.org/10.12737/2587-6295-2021-5-2-45-56>
4. Панфилов Г. О., Чугунов А. В. Централизация системы электронного гражданского участия в Российской Федерации: данные экспертных интервью // Управленческое консультирование. 2024. № 5. С. 253–264. <https://doi.org/10.22394/1726-1139-2024-5-253-264>
5. Evans-Pritchard E. E. The Nuer, a description of the modes livelihood and political institutions of a Nilotic people. Oxford: Clarendon Press. 1940.
6. Lipsky M. Toward a Theory of Street-level Bureaucracy. Madison, WI: Institute for Research on Poverty, University of Wisconsin, 1969. 46 p. (Institute for Research on Poverty Discussion Papers. No. 48).
7. Российский чиновник: социологический анализ жизненного мира государственных и муниципальных служащих / Под ред. Д.М. Рогозина. М.: ФГБУН Институт социологии РАН, 2015.
8. Кононенко П.Б. Информационная открытость парламентов субъектов Российской Федерации: экспериментальный анализ // Вестник Волгоградского государственного университета. 2015. №1 (31). С. 99-110.
9. Панфилов Г. О. Электронные порталы сообщений о проблемах в контексте централизации политики цифрового развития (на примере Санкт-Петербурга) // Социально-политические исследования. 2024. № 3 (24). С. 48-70. <http://dx.doi.org/10.20323/2658-428X-2024-3-24-48>.
10. Коваленко, Н. Н. Исследование проблемы борьбы с распространением борщевика Сосновского в России при помощи электронных цифровых сервисов // Управление информационными ресурсами: Материалы XXI Международной научно-практической конференции, Минск, 28 марта 2025 года. Минск: Академия управления при Президенте Республики Беларусь, 2025. С. 429-431.

УДК 32.019.52

**СРАВНИТЕЛЬНЫЙ АНАЛИЗ РОССИЙСКИХ ID-КАРТ ЖИТЕЛЕЙ В КОНТЕКСТЕ  
ПРЕДОСТАВЛЕНИЯ СОЦИАЛЬНОЙ ПОДДЕРЖКИ****Райц Валерий Андреевич**

Университет ИТМО

Кронверкский пр., 49, Санкт-Петербург, 197101, Россия

e-mail: varaits@itmo.ru

**Аннотация.** В докладе представлены промежуточные результаты пилотного исследования, проведенного в марте 2025 г., с целью обнаружения региональных практик цифровых сервисов, предполагающих применение ID-карт жителя для получения доступа к цифровым и нецифровым услугам. Автором обозначаются закономерности в отношении карт жителей с точки зрения предоставления сервисов населению.

**Ключевые слова:** ID-карта региона; экосистема цифровых сервисов; цифровые технологии; цифровые услуги.

**A COMPARATIVE ANALYSIS OF RUSSIAN RESIDENTS' ID CARDS  
IN THE CONTEXT OF PROVIDING SOCIAL SUPPORT****Raits Valeriy**The St. Petersburg National Research University of Information Technologies,  
Mechanics and Optics (University ITMO)

49 Kronverksky Av, St. Petersburg, 197101, Russia

e-mail: varaits@itmo.ru

**Abstract.** The report presents the interim results of a pilot study conducted in March 2025 to identify regional digital service practices involving the use of resident ID cards to gain access to digital and non-digital services. The author identifies patterns in relation to residents' maps in terms of providing services to the public.

**Keywords:** regional ID-cards; ecosystem of digital services; digital technologies; digital services.

В современной России в рамках реализации национальных целей развития до 2030 г. [1] вопросам социального обеспечения уделено особое внимание. В частности, одной из данных сфер выступает цифровая трансформация социальной среды. Согласно позиции исследователя, А. Нестеренко, цифровая трансформация представляет собой перечень действий, направленных на реализацию полномочий по предоставлению государственных услуг и выполнению государственных функций при помощи IT-активов [2]. Среди IT-активов стоит выделить следующие компоненты:

- цифровые технологии и информационные системы;
- сетевые устройства, позволяющие получать доступ к цифровым ресурсам;
- серверы и технологические модули, способствующие осуществлению функций по реализации цифровой трансформации системы [3].

Принимая во внимание широкий спектр способов внедрения цифровых технологий, с точки зрения предоставления социальных услуг необходимо выделить такой инструмент как «карта жителя» региона. Карта жителя (ID-карта жителя региона) представляет собой платежное средство, которое содержит совокупность цифровых сервисов внутри единой карты. В большинстве случаев, карта формируется на базе пластиковой карты платежной системы «МИР» банков России, однако существуют единичные примеры, не привязанных к этой национальной платежной системе (пример — «Карта москвича»). Преимуществом карты жителя выступает совмещение различных сервисов внутри единой системы, способных предоставить доступ к государственным

услугам, льготам или социальным пособиям держателям карты. Механизм предложения социально ориентированных сервисов в форме предоставления пособий или социальных выплат со стороны государственных учреждений осуществляется при помощи получения сведений о владельце карты жителя отдельного региона.

Исходя из направленности обеспечения социальными благами, можно выделить ряд положительных аспектов внедрения подобных механизмов в регионы России:

- наличие принципа адресности при предоставлении государством мер поддержки;
- усиленный контроль и эффективное расходование бюджета региона в части субсидирования средств нуждающимся гражданам страны [2].

Однако не стоит исключать возможностей возникновения кибер-рисков при использовании ID-карты. Наличие технических сбоев в результате кибератак или нестабильно отлаженной системы накладывает ряд ограничений по получению необходимых услуг в цифровом виде. Для этого требуется проведение комплексных мер со стороны государственных учреждений по предоставлению социальных услуг в бесперебойном режиме.

Согласно результатам проведенного обследования, открытых данных из информационных ресурсов 89 регионов РФ, было зафиксировано наличие 32 проектов карт жителей, распространяющих данный способ получения предпочтений [4–5]. По результатам веб-отсмotra региональных ID-карт, были обнаружены релевантные группы сервисов, сегментация которых осуществлялась по количеству сервисов, предоставляемых отдельной картой.

В частности, среди карт жителей прослеживается закономерность внедрения данных средств получения предпочтений по годам. Активное Внедрение ID-карт датируются 2021 (6 карт жителей) и 2024 (7 карт жителей) годами соответственно. Среди лидеров по предоставлению сервисов выделяются:

- «Единая карта Петербуржца» (13 сервисов);
- «Единая карта жителя Ямала «Морошка» (12 сервисов);
- «Единая карта Сахалинца» (10 сервисов).

В ходе первичного анализа стало известно, что в 14 регионах присутствия ID-карт есть мобильные приложения, которые содержатся в карте жителя региона. Среди проанализированных моделей ID-карт было зафиксировано существование уникальных сервисов для граждан. Например, «Единая карта Петербуржца» в качестве предпочтений предлагает «учет банных услуг» для льготных категорий граждан, а «Единая карта жителя Самарской области» дает возможность принять участие в проекте «Моя Третьяковка» с целью оказания помощи в виде пожертвования в филиал Третьяковской галереи, расположенной в Самаре.

Помимо непосредственных сервисов, которые предоставляет ID-карта, среди сервисов прослеживаются элементы геймификации, выраженные в получении некоего бонуса за определённые действия. Подобный механизм содержится в карте жителя Вологды под названием «городской бонус», благодаря которому владелец карты может обменять заработанные за участие в социально значимых мероприятиях баллы на конкретные бонусы.

Некоторые проанализированные карты жителей регионов содержат крайне небольшой функционал, либо позиционируются в качестве ID-карты при наличии только одного сервиса. В качестве примера можно привести карту жителя Республики Крым «Цифровая среда — Многофункциональная карта жителя Республики Крым» [6], в которой на данный момент содержится только функционал системы оплаты проезда в общественном транспорте.

По предварительным результатам анализа полученных данных можно сделать следующие выводы:

1. Среди основных сервисов подавляющего количества проанализированных ID-карт выступают банковские сервисы, сервисы по получению льгот и услуги социального обслуживания для держателей карт.
2. Наличие единичных компонентов внутри систем ID-карт снижают потенциальный эффект от подобных цифровых экосистемных сервисов.
3. В дальнейших исследованиях рекомендуется использовать качественные методы исследования для определения показателей результативности предоставляемых цифровых услуг населению при помощи ID-карт.

*Исследование выполнено за счет гранта № 23-18-20079 Российского научного фонда и Санкт-Петербургского научного фонда «Исследование социальной результативности электронного взаимодействия граждан и власти в Санкт-Петербурге на примере городских цифровых сервисов».*

#### СПИСОК ЛИТЕРАТУРЫ

1. Указ о национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года / Официальные сетевые ресурсы Президента России [Электронный ресурс]. URL: <http://www.kremlin.ru/acts/news/73986> (дата обращения: 11.08.2025).
2. Нестеренко, А. И. Оценка тенденций развития проекта «Карта жителя» в Республике Хакасия / А. И. Нестеренко, А. И. Макина // Вестник Хакасского государственного университета им. Н.Ф. Катанова. 2024. № 3(49). С. 99-104. EDN PZDLHI.
3. О порядке учета ИТ-активов, используемых для осуществления деятельности по цифровой трансформации системы государственного (муниципального) управления: Постановление Правительства РФ от 01.07.2024 № 900 // КонсультантПлюс: справочно-правовая система. URL: <http://publication.pravo.gov.ru/document/0001202407010028> (дата обращения: 11.08.2024).
4. Обновленная Карта жителя Приморья позволит получать соцвыплаты и скидки / Портал муниципального образования Артемовского городского округа [Электронный ресурс]. URL: [https://artemokrug.gosuslugi.ru/dlya-zhiteley/novosti-i-reportazhi/novosti-193\\_3927.html](https://artemokrug.gosuslugi.ru/dlya-zhiteley/novosti-i-reportazhi/novosti-193_3927.html) (дата обращения: 11.08.2025).
5. Петербуржцы сэкономили на поездках в транспорте по ЕКП сотни миллионов рублей / Официальный сайт АО «НСПК» [Электронный ресурс]. URL: <https://sbp.nspk.ru/smi/press-releases/d5ae6975-2605-4650-80f7-43159c9b9216> (дата обращения: 11.08.2025).
6. Распоряжение Совета министров Республики Крым от 15 апреля 2019 г. № 433-р «Об утверждении Концепции проекта «Многофункциональная карта жителя Республики Крым на 2019-2024 годы». [Электронный ресурс]. URL: <https://rk.gov.ru/documents/7ec7242d-4d60-40ba-82e6-c42a92e9c2fd> (дата обращения: 11.08.2025)..



## МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА «БЕЗОПАСНЫЕ ИНТЕЛЛЕКТУАЛЬНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ»

УДК 004.89:616.833.17

### МЕДИЦИНСКАЯ ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ДЛЯ ПЕРСОНАЛИЗИРОВАННОГО ВОССТАНОВЛЕНИЯ МИМИКИ ЛИЦА ПОСЛЕ ИНСУЛЬТА

**Авдеева Таисия Михайловна, Жаранова Анастасия Олеговна, Литвинов Владислав Леонидович**  
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевикова пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mails: tavdeeva-1@yandex.ru, zharanovaan@gmail.com, vlad.litvinov61@gmail.com

**Аннотация.** В работе представлен проект интеллектуальной информационной системы для персонализированных тренировок по восстановлению мимических мышц у пациентов после инсульта. Обоснована актуальность разработки системы, связанная с высокой заболеваемостью и дефицитом доступной реабилитации. Приведены функциональные требования, описана модульная архитектура системы. Охарактеризован нейросетевой модуль для классификации корректности выполнения упражнений и генерации вероятностной оценки для адаптации программы, основанный на методе Виолы-Джонса для распознавания лица и сверточной нейронной сети для анализа мимики. Обозначены перспективы разработки системы, основанные на AR-подсказках и модели прогнозирования сроков восстановления. Предложенное решение может повысить доступность и объективность реабилитации мимических мышц, сочетая практические инструменты реабилитации с методами компьютерного зрения и машинного обучения.

**Ключевые слова:** реабилитация после инсульта; мимические мышцы; интеллектуальная информационная система; компьютерное зрение; сверточные нейронные сети.

### MEDICAL INTELLIGENT SYSTEM FOR PERSONALIZED REHABILITATION OF FACIAL MUSCULATURE AFTER STROKE

**Avdeeva Taisiya, Zharanova Anastasia, Litvinov Vladislav**  
The Bonch-Bruевич Saint Petersburg State University of Telecommunications  
22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mails: tavdeeva-1@yandex.ru, zharanovaan@gmail.com, vlad.litvinov61@gmail.com

**Abstract.** This paper presents the design of an intelligent information system for personalized training aimed at restoring facial musculature in post-stroke patients. The relevance of the proposed system is motivated by the high incidence of stroke and the lack of accessible rehabilitation services. Functional requirements are specified and a modular system architecture is described. A neural-network module is characterized for classifying the correctness of exercise execution and generating probabilistic scores to adapt the training program; the module combines Viola-Jones face detection with a convolutional neural network for facial movement analysis. Future development directions include integration of augmented-reality guidance and predictive models for recovery timelines. The proposed solution can improve the accessibility and objectivity of facial muscle rehabilitation by combining practical rehabilitation tools with computer-vision and machine-learning methods.

**Keywords:** stroke rehabilitation; facial musculature; intelligent information system; computer vision; convolutional neural networks.

Инсульт — одна из главных причин инвалидности, приводящей к длительной утрате трудоспособности и социальной дезадаптации. Согласно статистике Минздрава России, ежегодно регистрируется 450–500 тысяч новых случаев, и у 60% пациентов сохраняются нарушения мимики, что приводит к трудностям в общении и социальной изоляции. При этом очередь на бесплатную реабилитацию может достигать 6 месяцев, а коммерческие услуги недоступны для значительной части населения, особенно в отдаленных регионах страны.

Стандартные методы восстановления мимики основаны на упражнениях, но не адаптированы под индивидуальные особенности пациентов [1]. Отсутствие регулярного доступа к специалистам, особенно в отдаленных регионах, и субъективная оценка прогресса ограничивают их эффективность. В связи с этим, разработка информационной системы для проведения персонализированных тренировок по восстановлению мимических мышц после инсульта может значительно улучшить процесс реабилитации.

Развитие интеллектуальных технологий в здравоохранении поддерживается государственной политикой: Указ Президента Российской Федерации от 21 июля 2020 г. № 474 «О национальных целях развития Российской

Федерации на период до 2030 года» задает стратегическую рамку цифровой трансформации, а Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» выделяет внедрение искусственного интеллекта в медицину как приоритет. Данные документы обосновывают актуальность разработки отечественных систем для дистанционной и персонализированной реабилитации после инсульта.

Анализ существующих систем реабилитации, включая Neofect, MindMotion GO, FaceSlim и MimicMe, позволил выявить несколько существенных ограничений. Основной проблемой является отсутствие специализации на восстановлении мимических мышц, поскольку эти платформы ориентированы преимущественно на общую двигательную реабилитацию, когнитивные функции или косметические задачи. Такой подход снижает их эффективность для пациентов с нарушениями мимики, нуждающихся в целенаправленной терапии.

Еще одним недостатком является зависимость многих систем от дорогостоящего оборудования, такого как VR-шлемы или сенсоры, что значительно ограничивает их доступность для широкого круга пациентов. Кроме того, большинство платформ слабо интегрированы с медицинскими специалистами, не предусматривая возможности удаленного контроля со стороны врачей. Подобное ограничение затрудняет своевременную коррекцию реабилитационных программ и мониторинг прогресса пациентов, что особенно важно для эффективного восстановления.

Современные исследования показывают активное внедрение искусственного интеллекта в постинсультную терапию — от ранней диагностики до долговременной реабилитации. Наблюдается рост интереса к домашним цифровым решениям с использованием сенсоров, VR/AR и компьютерного зрения [2, 3]; в то же время специализированные платформы для восстановления мимики остаются редкостью, что подтверждает актуальность предлагаемой разработки.

Основные функциональные требования к системе включают проведение тренировок мимических мышц с упражнениями, регистрацию врачей и пациентов с возможностью их взаимного прикрепления, отслеживание динамики восстановления и сохранение данных о тренировках.

Архитектура системы строится на взаимосвязанных модулях. Модуль авторизации отвечает за регистрацию и аутентификацию пользователей, разделяя роли врачей и пациентов. Модуль тренировок обеспечивает контроль выполнения упражнений с оценкой результатов через нейросетевые алгоритмы. Аналитический модуль собирает данные, формирует отчеты и визуализирует прогресс. Личные кабинеты врача и пациента предоставляют инструменты для управления реабилитационными программами, просмотра рекомендаций, анализа достижений и обмена информацией. Такая структура обеспечивает гибкость, масштабируемость и возможность поэтапной интеграции с клиническими системами.

Ключевым компонентом системы является нейросетевой модуль детекции лиц, реализованный с использованием метода Виолы-Джонса [4]. Он локализует лицо и выделяет релевантную область, а также выполняет предварительную обработку изображений для снижения размерности и повышения устойчивости модели. Для классификации корректности выполнения упражнения применяется бинарная сверточная нейронная сеть [5]. Архитектура сети включает слои Conv2D, MaxPooling2D, Flatten и Dense с сигмоидной функцией активации на выходе.

Для реализации системы выбран следующий технологический стек: Python (для серверной логики), PyQt5 (для разработки интерфейса), OpenCV и TensorFlow (для работы нейросетевого модуля), PostgreSQL (хранение данных).

В перспективах развития системы возможна интеграция AR-подсказок для коррекции упражнений в реальном времени, создание мобильного приложения, а также разработка моделей прогнозирования сроков восстановления мимических мышц на основе данных тысяч пациентов. Для подтверждения эффективности системы планируется партнерство с медицинскими центрами, что позволит провести клиническую валидацию и адаптировать решение под практические нужды.

Таким образом, разработка информационной системы для восстановления мимических мышц после инсульта представляет собой важный шаг к улучшению реабилитационного процесса. Предложенная интеллектуальная информационная система представляет собой интеграцию методов компьютерного зрения и машинного обучения с практическими инструментами реабилитации. Система направлена на повышение доступности и эффективности восстановления мимических мышц после инсульта посредством автоматизированной оценки, персонализации программ и дистанционного контроля.

#### СПИСОК ЛИТЕРАТУРЫ

1. Завалий Л.Б., Рамазанов Г.Р., Калантарова М.В., Рахманина А.А., Холмогорова А.Б., Петриков С.С. Нейропсихические принципы восстановительного обучения в терапии пациентов с нейропатией лицевого нерва. // Журнал им. Н.В. Склифосовского Неотложная медицинская помощь, 2022, №11 (3), С. 457-463.
2. Arntz A. Technologies in Home-Based Digital Rehabilitation: Scoping Review // JMIR Rehabilitation and Assistive Technologies. Vol 10. 2023. DOI: 10.2196/43615.
3. Kopallia S. R. Artificial intelligence in stroke rehabilitation: From acute care to long-term recovery // Neuroscience 572. 2025. P. 214-231. DOI: 10.1016/j.neuroscience.2025.03.017.
4. Viola, P. Robust real-time face detection / P. Viola, M.J. Jones // Journal of Computer Vision. 2004. Vol. 57(2) С. 137-154.
5. Багаев, И.И. Анализ понятий нейронная сеть и сверточная нейронная сеть, обучение сверточной нейросети при помощи модуля TensorFlow // Математическое и программное обеспечение систем в промышленной и социальной сферах. 2020. Т.8. № 1. С. 15-22.

УДК 004.8

**ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ПРЕДОТВРАЩЕНИЯ МОШЕННИЧЕСКИХ ТРАНЗАКЦИЙ****Асадуллаев Владислав Эдуардович, Филиппов Феликс Васильевич**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Большевики пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

e-mails: filippovfelix@gmail.com, 2vladik9602@gmail.com

**Аннотация.** Мошенничество с использованием цифровых каналов связи и платёжных инструментов становится всё более масштабным, изощрённым и автоматизированным. В условиях активного развития онлайн-банкинга, маркетплейсов, мобильных приложений и финансовых платформ, осуществляющих дистанционное обслуживание клиентов, формируется благоприятная среда для злоумышленников, стремящихся использовать уязвимости систем для незаконного обогащения. В работе рассмотрены основные проблемы, которые необходимо решить для построения эффективной системы предотвращения мошеннических транзакций. Предложена архитектура системы, включающая программные модули машинного обучения, реализующие механизмы обнаружения несанкционированных транзакций.

**Ключевые слова:** искусственный интеллект; финансовые транзакции; нейронные сети; информационная безопасность.

**INTELLIGENT SYSTEM FOR PREVENTING FRAUDULENT TRANSACTIONS****Asadullaev Vladislav, Filippov Felix**

The Bonch-Bruевич Saint Petersburg State University of Telecommunications,

22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia

e-mails: filippovfelix@gmail.com, 2vladik9602@gmail.com

**Abstract.** Fraud using digital communication channels and payment instruments is becoming increasingly large-scale, sophisticated and automated. In the context of the active development of online banking, marketplaces, mobile applications and financial platforms that provide remote customer service, a favorable environment is being formed for attackers seeking to exploit system vulnerabilities for illegal enrichment. The paper considers the main problems that need to be solved to build an effective system for preventing fraudulent transactions. The system architecture is proposed, including machine learning software modules that implement mechanisms for detecting unauthorized transactions.

**Keywords:** artificial intelligence; financial transactions; neural networks; information security.

Одним из примеров систем подобного назначения может служить FIS ANTIFRAUD [1], которая решает задачи, связанные с кредитными заявками. Широко развиваются кросс-канальные системы обнаружения и выявления мошеннических транзакций в режиме реального времени Smart Fraud Detection [2]. В обзорах [3, 4] представлены системы мирового и российского рынка систем антифрода. Рассмотренные в этих работах подходы показывают пути решения большинства проблем, стоящих в этой сфере. Однако разработка интеллектуальной системы предотвращения мошеннических транзакций связана еще со многими не решенными ключевыми проблемами, такими, например, как:

Сложность выявления новых схем мошенничества. Системы должны непрерывно обучаться на новых данных, чтобы обнаруживать ранее неизвестные паттерны.

Обработка больших объемов данных в реальном времени. Банковские транзакции требуют мгновенного анализа. Задержки в обработке могут привести к финансовым потерям.

Ложные срабатывания и их влияние на клиентов. Излишне строгие правила могут блокировать легитимные транзакции, вызывая недовольство клиентов. Баланс между безопасностью и удобством пользователей остается критической проблемой.

Для решения подобных проблем в основу предлагаемой системы положено использование нейронной сети, обучаемой на датасетах платёжных инструментов. Архитектура системы включает модули сбора, анализа и классификации транзакций. Кроме того, в ней используются средства интеграции с внешними API для реализации методов **гибкого масштабирования** архитектуры и механизмов повторного обучения на новых данных. Гибкое **масштабирование** системы подразумевает, в частности, дополнение или коррекцию бизнес-правил, обновление моделей и фичей, добавление внешних источников — черные списки, списки санкций, данные колл-центров.

**СПИСОК ЛИТЕРАТУРЫ**

1. Проверка и противодействие мошенничеству в банке. [Электронный ресурс]. URL: <https://fisgroup.ru/blog/antifraud-v-banke>. (дата обращения: 22.08.2025).
2. Антифрод-системы в борьбе с кредитным мошенничеством. [Электронный ресурс]. <https://ib-bank.ru/bisjournal/post/1886>. (дата обращения: 22.08.2025).
3. Обзор рынка систем противодействия мошенничеству. [Электронный ресурс]. [https://www.anti-malware.ru/analytics/Market\\_Analysis/Anti-Fraud](https://www.anti-malware.ru/analytics/Market_Analysis/Anti-Fraud). (дата обращения: 22.08.2025).
4. Васильев Т.И. Разработка и внедрение систем для борьбы с мошенничеством в финансовых транзакциях. Экономика. Информатика. 2024. Т.51, № 4 (919-925). DOI 10/52575.2687-0932-2024-51-4-919-925.

УДК 004.492.3

**ПРОТИВОДЕЙСТВИЕ АТАКАМ ТИПА HULK В ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ****Бабанов Захар Дмитриевич, Максименко Сергей Олегович, Шевченко Александр Александрович**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

e-mails: zach.fadeev@yandex.ru, mmickeys@bk.ru, alex\_pavel1991@mail.ru

**Аннотация.** Представлено исследование устойчивости ZigBee-сетей к распределённым атакам типа «отказ в обслуживании» (HULK), основанное на использовании методов машинного и подкрепляющего обучения. Предложенный подход сочетает анализ сетевого трафика с динамическим управлением ключами, что позволяет учитывать специфику IoT-протокола и ограниченные вычислительные ресурсы устройств. В ходе экспериментов в среде Mininet на реальном IoT-трафике показано, что комбинация алгоритмов Random Forest и KNN с элементами reinforcement learning обеспечивает точность выше 97% при сокращении задержек обработки на 40%. Полученные результаты демонстрируют перспективность интеграции интеллектуальных моделей в системы защиты ZigBee и подтверждают необходимость разработки специализированных решений для IoT-инфраструктур.

**Ключевые слова:** IoT; ZigBee; HULK; отказ в обслуживании; интеллектуальные методы; защита сетей.

**COUNTERING HULK-TYPE ATTACKS IN INFORMATION AND COMPUTING NETWORKS****Babanov Zach, Maksimenko Sergey, Shevchenko Aleksandr**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia

e-mails: zach.fadeev@yandex.ru, mmickeys@bk.ru, alex\_pavel1991@mail.ru

**Abstract.** This paper presents a study of ZigBee network resilience against distributed denial-of-service (HULK) attacks using machine learning and reinforcement learning techniques. The proposed approach combines traffic analysis with dynamic key management, taking into account the specifics of the IoT protocol and the limited computational resources of devices. Experiments conducted in the Mininet environment with real IoT traffic demonstrated that a combination of Random Forest and KNN algorithms, enhanced with reinforcement learning, achieves an accuracy above 97% while reducing processing latency by 40%. The results highlight the potential of integrating intelligent models into ZigBee defense mechanisms and confirm the need for specialized solutions tailored to IoT infrastructures.

**Keywords:** IoT; ZigBee; HULK; denial-of-service; intelligent methods; network protection.

Рост количества подключённых IoT-устройств делает их привлекательной целью для атак типа «отказ в обслуживании». Среди них особое внимание привлекает HULK-атака, генерирующая множество уникальных HTTP-запросов и тем самым обходящая традиционные фильтры. Применение такого подхода к ZigBee-сетям приводит к перегрузке шлюза, истощению батарейных узлов и блокировке легитимного трафика [1-5].

Предложенный метод защиты ориентирован на специфику ZigBee, которая характеризуется низкой пропускной способностью, предсказуемыми циклами опроса датчиков и ограниченными вычислительными ресурсами. Для анализа применялось шесть ключевых характеристик сетевого трафика, описывающих интенсивность потоков и статистику пакетов. На их основе были построены модели классификации с использованием SVM, Random Forest, Naive Bayes и KNN. Дополнительно применена схема reinforcement learning для динамического управления ключами, что позволило снизить вероятность успешного проведения атаки [6-8].

Эксперименты в среде Mininet на трафике десяти IoT-устройств подтвердили эффективность предложенной методики. Лучшие результаты показали RF и KNN, достигнув точности свыше 97% и F1-метрика порядка 98%. Интеграция reinforcement learning обеспечила дополнительное сокращение задержек при обработке пакетов и снизила нагрузку на устройства. При этом срок службы батарей увеличился почти на одну пятую за счёт оптимизации частоты опроса [9-12].

Результаты исследования сопоставимы с передовыми методами в области защиты сетей, однако предложенный подход отличается ориентацией на ограничения IoT-протоколов. В отличие от решений, разработанных для SDN или облачных инфраструктур, методика учитывает энергопотребление устройств и особенности передачи данных в ZigBee. Это делает её применимой для практической защиты умных домов, медицинских и промышленных IoT-систем [13].

Несмотря на достигнутые результаты, остаются направления для совершенствования, включая оптимизацию reinforcement learning для слабых устройств, расширение набора исследуемых атак и проверку масштабируемости метода. Тем не менее, проведённые эксперименты показали, что интеллектуальные методы, адаптированные под специфику IoT-протоколов, могут существенно повысить устойчивость ZigBee-сетей к HULK-атакам и аналогичным угрозам.

**СПИСОК ЛИТЕРАТУРЫ**

1. Idhammad M., Afdel K., Belouch M. Detection System of HTTP DDos Attacks in a Cloud Environment Based on Information Theoretic Entropy and Random Forest // Security and Communication Networks. 2018. С. 1–13.
2. Vancin S., Erdem E. Design and Simulation of Wireless Sensor Network Topologies Using the ZigBee Standard // International Journal of Computer Networks and Applications (IJCA). 2015. Т. 2, № 3. С. 135–143.

3. de Lima Filho F. S., Silveira F. A. F., Brito Junior A. M., Vargas-Solar G., Silveira L. F. Smart Detection: An Online Approach for DoS/DDoS Attack Detection Using Machine Learning // Security and Communication Networks. 2019. С. 1–15.
4. Breiman L., Cutler A. Random Forests [Электронный ресурс]. URL: [https://www.stat.berkeley.edu/~breiman/RandomForests/cc\\_home.htm](https://www.stat.berkeley.edu/~breiman/RandomForests/cc_home.htm) (дата обращения: 30.04.2024).
5. Sitawan D., Sandra S., Alzahrani E., Budiarto R. Comparative Analysis of K-Means Method and Naive Bayes Method for Brute Force Attack Visualization // 2017 2nd International Conference on Anti-Cyber Crimes (ICACC). Abha, Saudi Arabia, 2017. С. 177–182.
6. Neto E., Dadkhah S., Ghorbani A.A. et al. IoT Zigbee device security: A comprehensive review. Internet of Things. 2023.
7. Critical Flaw IDed In ZigBee Smart Home Devices // Cognosec URL: [http://cognosec.com/zigbee\\_exploited\\_8F\\_Ca9.pdf](http://cognosec.com/zigbee_exploited_8F_Ca9.pdf) (дата обращения: 30.04.2025)
8. Липатников В. А., Шевченко А.А. Методика проактивного управления информационной безопасностью распределенной информационной системы на основе интеллектуальных технологий // Информационные системы и технологии. 2022. № 2(130). С. 107–115.
9. Липатников В. А., Шевченко А.А. Математическая модель процесса управления информационной безопасностью распределенной информационной системы в условиях несанкционированного воздействия злоумышленника // Информационные системы и технологии. 2022. № 3(131). С. 121–130.
10. Липатников В.А., Шевченко А.А., Мелехов К.В., Задбоев В.А. Метод активной защиты объектов критической информационной инфраструктуры от кибератак на основе прерывания процесса воздействия нарушителя // Информационно-управляющие системы. 2025. № 2(135). С. 37–49.
11. Защищенная модель программно-определяемой сети в среде виртуализации KVM / Д. В. Сахаров, А. В. Красов, И. А. Ушаков, Г. А. Орлов // Электросвязь. 2020. № 3. С. 26–32. DOI 10.34832/ELSV.2020.4.3.004. EDN IRRVAB.
12. Ушаков, И. А. Методика обнаружения аномалий в сетевом трафике с использованием IPS на основе Security Onion / И. А. Ушаков, А. В. Красов, Д. Д. у. Мулладжанов // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2022. № 1. С. 5–11. DOI 10.46418/2079-8199\_2022\_1\_1. EDN DSQOHV.
13. Идея и общая концепция применения мультиагентного подхода к созданию крупномасштабных интеллектуальных систем обнаружения вторжений / С. И. Штеренберг, А. В. Красов, В. В. Максимов, А. В. Архипов // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2023. № 3. С. 128–136. DOI 10.46418/2079-8199\_2023\_3\_20. EDN YFDWIK.

УДК 004.056

### АДАПТИВНАЯ ДЕЦЕНТРАЛИЗОВАННАЯ ПЕРЕДАЧА ДАННЫХ С ФРАГМЕНТАРНЫМ ШИФРОВАНИЕМ, МУЛЬТИ-МАРШРУТИЗАЦИЕЙ И СЕКТОРНОЙ АДРЕСАЦИЕЙ

Горохов Дмитрий Геннадьевич, Лабковская Римма Яновна

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mails: rimma.labkovskaya@gmail.com, harokhau.opt.stack@gmail.com

**Аннотация.** Представляется теоретическая концепция децентрализованной передачи данных, совмещающая фрагментарное шифрование, адаптивную мульти-маршрутизацию и секторную (кластерную) адресацию. Описывается метод распределения полезной нагрузки на криптографические независимые фрагменты, передающиеся по различным путям локально-оптимальным выбором следующего узла связи. Мотивируется научная новизна интеграции механизмов работы децентрализованной передачи данных в единую архитектурную схему и определения верифицируемых метрик приватности и устойчивости передачи данных. Описывается практическая значимость адаптивной децентрализованной передачи данных с фрагментарным шифрованием, мульти-маршрутизацией и секторной адресацией для снижения эффективности трафик-анализа и устойчивости к частичным отказам в процессе передачи данных.

**Ключевые слова:** децентрализованные сети; фрагментарное шифрование; мульти-маршрутизация; P2P; секторная адресация.

### ADAPTIVE DECENTRALIZED DATA TRANSMISSION WITH FRAGMENTED ENDCRYPTION, MULTI-ROUTING AND SECTOR ADDRESSING

Harokhau Dzmitry, Labkovskaya Rimma

The Bonch-Bruевич Saint Petersburg State University of Telecommunications  
22 Bolshevnikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mails: rimma.labkovskaya@gmail.com, harokhau.opt.stack@gmail.com

**Abstract.** A theoretical concept of decentralized data transmission is presented, combining fragmentary encryption, adaptive multi-routing, and sector (cluster) addressing. It describes a method for distributing payloads into cryptographically independent fragments that are transmitted via different paths by locally optimal selection of the next communication node. It motivates the scientific novelty of integrating decentralized data transmission mechanisms into a unified architectural scheme and defining verifiable metrics of privacy and data transmission stability. The practical significance of adaptive decentralized data transmission with fragmentary encryption, multi-routing, and sector addressing for reducing the effectiveness of traffic analysis and resistance to partial failures in the data transmission process is described.

**Keywords:** decentralized networks; fragmentary encryption; multi-routing; P2P; sector addressing.

Традиционные централизованные архитектуры передачи данных уязвимы к единой точке отказа и глобальному мониторингу, что стимулировало развитие децентрализованных сетей и одноранговых схем маршрутизации для повышения устойчивости и приватности коммуникаций [1]. В рамках описываемой концепции ключевой акцент делается на совмещении трех механизмов: фрагментарного шифрования полезной нагрузки, адаптивной мульти-маршрутизации по нескольким путям и секторной адресации, создающей групповую анонимность получателя. Такая композиция направлена на одновременное снижение информативности отдельно перехваченных единиц трафика,

декорреляцию наблюдаемых маршрутов и устранение прямой связи «пакет-получатель», характерной для классических адресных схем.

Метод распределения полезной нагрузки начинается с криптографической фрагментации: исходное сообщение делится на фрагменты, каждый из которых шифруется отдельным производным ключом и снабжается независимой меткой целостности, что делает любой единичный фрагмент информационно бесполезным для криптоанализа и снижает риски при частичном перехвате [2]. Для обеспечения восстановимости в условиях потерь предложено использовать схемы кодов со стираниями, позволяющие реконструировать сообщение из подмножества фрагментов при соблюдении порога достаточности, что согласуется с теоретическими основами представления данных в системах остатков и с практикой построения устойчивых распределенных хранилищ. Такой подход дополняется локально-оптимальным выбором следующего узла связи для каждого фрагмента, при котором решения о маршрутах принимаются на основе телеметрии о задержках, потерях и надежности соседних узлов, что соответствует современным подходам к интеллектуально-адаптивному управлению сетевым трафиком [3].

Адаптивная мульти-маршрутизация разворачивает доставку каждого фрагмента по нескольким альтернативным путям, позволяя динамически перераспределять нагрузку и обходить деградирующие участки сети. Дополнительно, локальная политика узла переобучается по мере накопления наблюдений, сохраняя ограниченное знание о глобальной топологии и тем самым уменьшая поверхность утечки метаданных. Переход от статичных к адаптивным схемам маршрутизации обоснован как с точки зрения эффективности, то есть снижение перегрузок и задержек, так и с точки зрения безопасности: постоянная ротация путей и асинхронное поступление фрагментов ухудшают результаты корреляционного трафик-анализа при частичном наблюдении каналов [4]. В совокупности это создает контролируемый компромисс «приватность-задержка-накладной трафик», где увеличение числа путей и интенсивность ротации маршрутов повышают стойкость к анализу, но требуют калибровки, чтобы не привести к избыточным расходам и росту латентности.

Секторная адресация завершает архитектурную схему: вместо явного адреса указывается логический сектор — группа узлов, выделенная по топологии, географии или доверительным признакам. Фрагменты рассылаются в сектор таким образом, что каждый участник получает только часть данных, а полная реконструкция доступна исключительно целевому получателю, имеющему соответствующий ключевой материал и индекс отбора фрагментов. Такой групповой способ доставки создает слой анонимности адресата: для наблюдателя сектор выступает множеством равновероятных кандидатов, а вероятность однозначной идентификации ограничена размером кластера и снижается при росте разноса маршрутов между фрагментами. Дополнительная политика удаления следов — автоматическое удаление временных фрагментов у нецелевых узлов со временем или после подтверждения сборки [5].

Научная новизна концепции состоит не в изоляции отдельных механизмов, а в их интеграции в единую архитектурную схему с формализуемыми свойствами и метриками: независимая крипто-фрагментация, адаптивная мульти-маршрутизация и секторная адресация совместно обеспечивают снижение взаимной информации между источником и наблюдениями на контролируемых линиях и ограничение вероятности деанонимизации адресата верхней оценкой через размер сектора и наблюдаемую долю путей. Теоретические обоснование восстановимости опирается на коды со стираниями и соответствующие MDS-границы, оценка приватности на моделях трафик-анализа и взаимной информации, а устойчивость на вероятных характеристиках распределения потерь и деградаций каналов в распределенных системах [6]. Описываемая триада задает основу для симуляционной валидации: варьируя размер сектора, уровень избыточности, число маршрутов и долю наблюдаемых узлов, можно измерять долю успешно восстановленных сообщений, медианную задержку и дисперсию, прирост накладного трафика, вероятность деанонимизации при наилучшем корреляционном алгоритме и объем резидуальных данных до и после удаления.

Практическая значимость такого подхода проявляется в сценариях, где критичными являются приватность и отказоустойчивость: корпоративные сети без единой точки отказа, защищенный документооборот без доверенного посредника, коммуникация в средах с нестабильными каналами, а также системы интернета вещей, где параллельная обработка крипто-фрагментов снижает требования к ресурсам на узлах. По сравнению с классическими одноранговыми решениями и анонимными маршрутизаторами, предлагаемый каркас делает ставку на измеримый эффект: меньшая коррелируемость трафика, групповая анонимность получателя и гарантированная реконструкция при частичных потерях, при этом компромиссные накладные расходы поддаются настройке политиками мульти-маршрутизации и размерами секторов [7]. В результате формируется дорожная карта реализации: сначала формальная модель и спецификация форматов сообщений, затем событийная симуляция с отчетом по метрикам, а в дальнейшем минимальный прототип для демонстрации корректности фрагментации, сборки и поведенческих свойств маршрутизатора политики.

## СПИСОК ЛИТЕРАТУРЫ

1. Кушнарев А. Альтернативный интернет: что это такое и как он работает // РБ.РУ. 2023. [Электронный ресурс]. URL: <https://rb.ru/columns/alternativnyj-internet/> (дата обращения: 29.08.2025).
2. Ишкватов С. М. Способ и алгоритм определения типа трафика в зашифрованном канале связи // Труды учебных заведений связи. 2022. Т. 8. № 4. С. 109–118. [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/sposob-i-algoritm-opredeleniya-tipa-trafika-v-shifrovannom-kanale-svyazi> (дата обращения: 29.08.2025).
3. Рекомендация МСЭ-Т X.1362. Простая процедура шифрования для среды интернета вещей (IoT). Женева: МСЭ, 2017. 32 с.
4. Шифрование Azure — общие сведения // Microsoft Learn. 2025. [Электронный ресурс]. URL: <https://learn.microsoft.com/ru-ru/azure/security/fundamentals/encryption-overview> (дата обращения: 29.08.2025).
5. ProstoKirReal. Сложно о простом. Самые популярные протоколы и принципы их работы. HTTP, HTTPS, SSL и TLS. Часть 3 // Хабр. 2024. 25 дек. [Электронный ресурс]. URL: <https://habr.com/ru/companies/timeweb/articles/857298/> (дата обращения: 29.08.2025).
6. Шесть устройств для сетевого шифрования: плюсы и минусы. СПб. 2020. [Электронный ресурс]. URL: <https://systempb.ru/company/articles/shest-ustroystv-dlya-setevogo-shifrovaniya-plyusy-i-minusy/> (дата обращения: 29.08.2025).



УДК 004.8

**ОЦЕНКА ЭФФЕКТИВНОСТИ СИСТЕМ МОНИТОРИНГА И УПРАВЛЕНИЯ  
ИНФОРМАЦИОННЫМИ СЕТЯМИ В УСЛОВИЯХ ДИНАМИЧЕСКИ  
МЕНЯЮЩЕЙСЯ НАГРУЗКИ И ТРЕБОВАНИЙ ПОЛЬЗОВАТЕЛЕЙ****Губин Александр Николаевич, Климова Юлия Вячеславовна**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевикова пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mails: gan50\_60@mail.ru, yuly.klim@gmail.com

**Аннотация.** В статье рассматриваются основные современные подходы к мониторингу и управлению информационными сетями, особенно в условиях динамично изменяющихся условий функционирования систем. Проводится анализ существующих систем мониторинга и определяются оценки эффективности таких систем. Рассматриваются различные подходы к решению задач адаптации систем мониторинга к изменениям условий их функционирования. Исследование основано на данных, характеризующих свойства систем мониторинга, используемых для решения практических задач, что подтверждает актуальность исследований. В заключении предлагаются рекомендации по выбору систем мониторинга и управления исходя из требований к задачам адаптации систем к изменениям условий их функционирования.

**Ключевые слова:** информационные сети; мониторинг; оценка эффективности.

**ASSESSMENT OF THE EFFECTIVENESS OF INFORMATION NETWORK MONITORING  
AND MANAGEMENT SYSTEMS IN THE CONTEXT OF DYNAMICALLY  
CHANGING USER LOADS AND REQUIREMENTS****Gubin Alexander, Klimova Julia**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications  
22 Bolshhevikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mails: alex.gubin50@mail.ru, yuly.klim@gmail.com

**Abstract.** The article examines the main modern approaches to monitoring and management of information networks, especially in the context of dynamically changing operating conditions of systems. An analysis of existing monitoring systems is carried out and estimates of the effectiveness of such systems are determined. Various approaches to solving the problems of adapting monitoring systems to changes in their operating conditions are considered. The study is based on data characterizing the properties of monitoring systems used to solve practical problems, which confirms the relevance of the research. In conclusion, recommendations are offered on the choice of monitoring and control systems based on the requirements for the tasks of adapting systems to changes in their operating conditions.

**Keywords:** information networks; monitoring; efficiency assessment.

В постоянно развивающемся мире ИТ-инфраструктур и окружений мониторинг имеет решающее значение для поддержания непрерывности и требуемого уровня качества работы информационных сетей и сервисов [1].

К основным задачам мониторинга информационных сетей относятся [2, 3]:

Анализ производительности сети в режиме реального времени.

- Измерение времени отклика сети при изменении условий функционирования.
- Диагностирование проблем, наблюдаемых в сети, путём мониторинга её поведения и сравнения его с обычным режимом работы.
- Отслеживание сетевого трафика и эффективность использования оборудования сети.
- Кроме того, некоторые пакеты сетевого мониторинга также выполняют мониторинг соглашений об уровне и качестве обслуживания запросов.

Для проведения сравнительной оценки систем мониторинга информационных сетей с точки зрения возможного изменения требований пользователя, можно использовать критерии, такие как гибкость, адаптивность, масштабируемость, поддержка интеграций и возможность настройки.

Окончательный выбор системы мониторинга зависит не только от результатов оценки эффективности системы мониторинга, но и от специфических требований организации. Если гибкость и адаптивность являются приоритетом, лучше рассмотреть системы с открытым исходным кодом, такие как Zabbix и Prometheus. Если важна простота использования и быстрая интеграция, то возможными кандидатами для выбора системы мониторинга станут SolarWinds NPM или PRTG.

**СПИСОК ЛИТЕРАТУРЫ**

1. Топ лучших инструментов для мониторинга сети в 2024 году. [Электронный ресурс]/ URL: <https://itshaman.ru/articles/4200/7-luchshikh-instrumentov-dlya-monitoringa-seti-v-2024-godu/> (дата обращения: 22.08.2025).
2. Новые подходы и новые возможности по мониторингу сетевой инфраструктуры. [Электронный ресурс]/ URL: <https://www.securityvision.ru/blog/novye-podkhody-i-novye-vozmozhnosti-po-monitoringu-setevoy-infrastruktury/> (дата обращения: 22.08.2025).
3. Обзор лучших программ для мониторинга сети в 2025 — Импортзамещение — Сравнение российской программы и иностранных аналогов. [Электронный ресурс]. URL: <https://www.10-strike.ru/network-monitor/obzor-analogov.shtml/> (дата обращения: 22.08.2025).

УДК 004.8

**ИНФОРМАЦИОННАЯ ЭФФЕКТИВНОСТЬ СИСТЕМ ПОДДЕРЖКИ ИТ-ПРОЕКТОВ****Литвинов Владислав Леонидович, Орлова Валерия Игоревна**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Большевикова пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

e-mails: vlad.litvinov61@gmail.com, cl.ler@yandex.ru

**Аннотация.** Рассматривается класс систем поддержки принятия решений в области менеджмента ИТ-проектов. Эффективность таких систем можно оценить по изменению исходной информационной энтропии в процессе выработки решения. В работе предлагается подход к количественной оценке информационной эффективности систем поддержки принятия решений, основанный на понятии Колмогоровской сложности и расстояния (дивергенции) Кульбака-Лейблера.

**Ключевые слова:** интеллектуальная система поддержки принятия решений; информационная эффективность; энтропия; Колмогоровская сложность; расстояние Кульбака-Лейблера.

**INFORMATION EFFICIENCY OF IT-PROJECT SUPPORT SYSTEMS****Litvinov Vladislav, Orlova Valery**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

22 Bolshhevikov Av, bldg 1, St. Petersburg, 193232, Russia

e-mails: vlad.litvinov61@gmail.com, cl.ler@yandex.ru

**Abstract.** The class of decision support systems in the field of IT project management is considered. The effectiveness of such systems can be assessed by changing the initial information entropy in the decision-making process. The paper proposes an approach to quantifying the information efficiency of decision support systems based on the concept of Kolmogorov complexity and Kullback-Leibler distance (divergence).

**Keywords:** intelligent decision support system; entropy; Kolmogorov complexity; Kullback-Leibler divergence.

Проектирование интеллектуальных систем поддержки принятия решений (СППР) требует формализации описания предметной области, что может быть сделано средствами онтологического подхода [1]. При проектировании реализуется принцип эволюционного развития, при котором сначала формируется топология системы, затем выбираются структуры связей и, наконец, оптимизируются параметры. Одним из подходов, который может быть применен для параметрической идентификации интеллектуальных систем поддержки принятия решений, — использование методов оценки информационной эффективности [2, 3]. В работе задача сформулирована в общем виде следующим образом.

Процесс извлечения полезной информации из входных данных базируется на использовании априорной информации как о статистических характеристиках входного множества, так и характеристиках выходных данных, подлежащих воспроизведению. Причем, очевидно, что чем больше такой информации используется при реализации СППР, тем эффективнее решается задача извлечения полезных данных. В общем случае, очевидно, имеется взаимосвязь между взаимной информацией и условными Колмогоровскими сложностями [2] при взаимодействии объектов (входной сигнал — информационная система — выходной сигнал).

Очевидно, что чем больше априорной информации о параметрах входных данных  $x$  и подлежащих выделению данных  $y$  используется при определении параметров информационной системы  $z$ , тем эффективнее будет решаться задача выделения  $y$ .

В работе [1] показано, что можно получать достаточно точные оценки Колмогоровской сложности на базе автокодировщиков, которые можно использовать для оценки информационной эффективности. Основной принцип работы и обучения автокодировщика — получить на выходном слое отклик, наиболее близкий к входному. С их помощью решается широкий спектр задач, и они представляют, пожалуй, лучший и наиболее адекватный образец для оценки информационной эффективности на базе Колмогоровской сложности. Практические примеры использования подобной модели позволяют объединить вероятностные определения энтропии, использованные выше, с алгебраической концепцией, введенной Колмогоровым [2]. Например, при решении задачи понижения размерности, сжатый образ  $h$  входного объекта  $x$  можно использовать для оценки энтропии.

В данной работе предлагается один из способов интерпретации оценки качества реконструкции как задачи минимизации расстояния Кульбака-Лейблера [1]. По сути, минимизация расстояния Кульбака-Лейблера в точности соответствует минимизации перекрёстной энтропии между распределениями.

Таким образом, предложенные подходы к оценке информационной эффективности могут быть полезны при построении систем поддержки ИТ-проектов и выбора наиболее эффективного варианта практической реализации.

**СПИСОК ЛИТЕРАТУРЫ**

1. Губин А.Н., Литвинов В.Л., Филиппов Ф.В. Информационная эффективность интеллектуальных систем поддержки принятия решений // В сборнике: Информационные системы и технологии в моделировании и управлении. Сборник трудов V Международной научно-практической конференции. Отв. редактор К.А. Маковейчук. 2020. С. 19-23.
2. Колмогоров А. Н. Три подхода к определению понятия «количество информации» // Проблемы передачи информации. 1965. Т. 1. № 1. С. 3-11.
3. Верещагин Н. К. Колмогоровская сложность и алгоритмическая случайность / Н. К. Верещагин, В. А. Успенский, А. Шень. М.: МЦНМО, 2013. 576 с.

УДК 004.8

## ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ОБРАЗОВАНИИ: ЭТИЧЕСКИЕ ВОПРОСЫ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Литвинов Владислав Леонидович, Самбунова Варвара Петровна

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевикова пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mails: vlad.litvinov61@gmail.com, varvara.sambu@gmail.com

**Аннотация.** Внедрение больших языковых моделей (LLM) в образовательный процесс (LLM4EDU) несет не только трансформационный потенциал, но и серьезные риски информационной безопасности. В работе рассмотрены ключевые проблемы, которые можно сгруппировать в несколько категорий: конфиденциальность и приватность данных, генерация небезопасного контента, манипуляции и академическая недобросовестность, уязвимости моделей и атаки. Показано, что безопасное применение LLM4EDU требует не просто технологического внедрения, а комплексного подхода, включающего строгую политику данных, технические меры защиты, контроль выводов модели и формирование цифровой культуры среди учащихся и преподавателей.

**Ключевые слова:** искусственный интеллект; образование; большие языковые модели; информационная безопасность.

## ARTIFICIAL INTELLIGENCE IN EDUCATION: ETHICAL ISSUES AND INFORMATION SECURITY

Litvinov Vladislav, Samburova Varvara

The Bonch-Bruevich Saint Petersburg State University of Telecommunications  
22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mails: vlad.litvinov61@gmail.com, varvara.sambu@gmail.com

**Abstract.** The introduction of large language models (LLM) into the educational process (LLM4EDU) carries not only transformational potential, but also serious information security risks. The paper considers key issues that can be grouped into several categories: confidentiality and privacy of data, generation of unsafe content, manipulation and academic dishonesty, vulnerabilities of models and attacks. It is shown that the safe use of LLM4EDU requires not just technological implementation, but an integrated approach, including strict data policy, technical protection measures, control of model conclusions and the formation of a digital culture among students and teachers.

**Keywords:** artificial intelligence; education; large language models; information security.

Одним из ярких примеров применения искусственного интеллекта в образовании стали большие языковые модели [1]. За последние несколько лет сформировался отдельный термин LLM4EDU (Large Language Models in Education, Большие языковые модели в образовании). LLM4EDU уже сегодня могут активно использоваться в разных сферах образовательной деятельности [2, 3]: создание образовательного контента, межкультурное общение, планирование карьеры, персонализированное обучение, подготовка к занятиям и экзаменам.

Однако, внедрение больших языковых моделей в образовательный процесс несет и серьезные риски информационной безопасности, а также проблемы этического характера. В работе выделены ключевые проблемы, которые можно сгруппировать в несколько категорий:

Конфиденциальность и приватность данных — наиболее острая проблема. Модели, обученные на данных учащихся, могут непреднамеренно запоминать и раскрывать конфиденциальную информацию в своих ответах третьим лицам. Существует риск утечек через промпты, а также риск несанкционированного доступа к базовым данным. Генерация небезопасного контента. LLM могут выдавать вредоносный, предвзятый, недостоверный или неподходящий для возраста контент (например, связанный с насилием, дискриминацией). Это требует сложной и непрерывной модерации.

Манипуляции и академическая недобросовестность. Упрощение создания качественного плагиата, написание эссе и решение задач без понимания материала учениками. Это ставит под угрозу саму цель обучения и оценку знаний.

Уязвимости моделей и атаки. Модели подвержены специфическим атакам, таким как инъекция промптов (подмена инструкций), извлечение тренировочных данных и «отравление» данных на этапе обучения, что может скомпрометировать всю систему в целом.

Таким образом, для преодоления указанных проблем требуется комплексный подход, включающий в себя строгую политику данных, технические меры защиты, контроль выводов модели, а главное — формирование цифровой культуры среди учащихся и преподавателей.

## СПИСОК ЛИТЕРАТУРЫ

1. Влияние ИИ на образование. [Электронный ресурс]. URL: <https://d-economy.ru/analitic/vlijanie-ii-na-obrazovanie/> (дата обращения: 22.08.2025).
2. Литвинов В.Л., Литвинова Е.В. Проблемы и тенденции применения генеративного искусственного интеллекта в образовании // Современное образование: содержание, технологии, качество. 2024. Т. 1. С. 107-109.
3. Муртузалиева Т.В., Цветкова А.Б. Искусственный интеллект как новая технология в обучении маркетологов // Экономические системы. 2025. Т. 18. № 2. С. 69-80.

УДК 004.9

## ПРИМЕНЕНИЕ ДИСТАНЦИОННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ОБУЧЕНИИ ГРАНТОВОЙ ДЕЯТЕЛЬНОСТИ

Литвинов Владислав Леонидович<sup>1</sup>, Литвинова Екатерина Владимировна<sup>2</sup>

<sup>1</sup> Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

<sup>2</sup> Ленинградский областной институт развития образования  
Чкаловский пр., 25, лит. А, Санкт-Петербург, 197136, Россия  
e-mails: vlad.litvinov61@gmail.com, ekalitinova@yandex.ru

**Аннотация.** Статья посвящена анализу опыта использования системы дистанционного обучения Moodle для реализации программы повышения квалификации педагогических работников в области грантовой деятельности. На примере программы «Технологии разработки и оформления грантовых проектов в сфере образования» рассматриваются возможности платформы для организации смешанного обучения, отработки практических навыков и преодоления типичных проблем, связанных с участием в грантовых конкурсах. Приводятся данные входной и итоговой диагностики, демонстрирующие эффективность использования LMS Moodle для формирования профессиональных компетенций педагогов.

**Ключевые слова:** LMS Moodle; повышение квалификации; грантовая деятельность; дистанционное обучение; смешанное обучение; проектная деятельность; профессиональное развитие.

## APPLICATION OF DISTANCE LEARNING TECHNOLOGIES IN GRANT WRITING TRAINING

Litvinov Vladislav<sup>1</sup>, Litvinova Ekaterina<sup>2</sup>

<sup>1</sup> The Bonch-Bruevich Saint Petersburg State University of Telecommunications  
22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia

<sup>2</sup> Leningrad Regional Institute for Educational Development  
25 Chkalovskiy Av, lit. A, St. Petersburg, 197136, Russia  
e-mails: vlad.litvinov61@gmail.com, ekalitinova@yandex.ru

**Abstract.** The article analyzes the experience of using the Moodle distance learning system to implement a professional development program for teachers in the field of grant activities. Using the example of the program «Technologies for the development and registration of grant projects in the field of education», the possibilities of a platform for organizing blended learning, developing practical skills and overcoming typical problems associated with participation in grant competitions are considered. The data of the input and final diagnostics are presented, demonstrating the effectiveness of using LMS Moodle for the formation of professional competencies of teachers.

**Keywords:** LMS Moodle; professional development; grant activities; distance learning; blended learning; project activities; professional development

Современные вызовы в системе образования, включая необходимость участия в грантовых конкурсах для привлечения дополнительного финансирования и реализации инновационных проектов, обуславливают потребность в эффективных программах повышения квалификации работников. В этом контексте особую актуальность приобретает использование систем дистанционного обучения, таких как LMS Moodle, которые позволяют организовать гибкий и доступный образовательный процесс, сочетающий теоретическую подготовку и практическую отработку навыков [1].

В рамках государственного задания ГАОУ ДПО «ЛОИРО» на 2025 год была разработана и реализована программа повышения квалификации «Технологии разработки и оформления грантовых проектов в сфере образования» объемом 72 часа. Программа была реализована в формате смешанного обучения с использованием LMS Moodle. Структура программы включала:

– Теоретические модули (20%): видеолекции, презентации, нормативные документы, размещенные в LMS Moodle.

– Практические занятия и самостоятельную работу (80%): интерактивные задания, форумы, мастермайнд (формат регулярных групповых встреч, где участники обмениваются опытом, идеями и знаниями для решения проблем, достижения целей и взаимной поддержки, находясь в роли равных), разбор кейсов и разработка проектных документов с использованием инструментов платформы [2].

Актуальность реализации данной программы была обусловлена необходимостью привлекать руководителей образовательных организаций и педагогических работников к участию в грантовых конкурсах различной направленности. Данная необходимость объясняется несколькими факторами.

Первым фактором можно назвать финансовую поддержку инновационных проектов. Гранты позволяют привлечь дополнительные средства на реализацию образовательных проектов и инициатив, которые невозможно финансировать в рамках стандартного бюджета.

Не менее важным фактором является повышение профессионального уровня педагогов в результате участия в грантовых конкурсах. Педагоги, участвующие в такой деятельности, показывают готовность к освоению новых технологий и методик. У них более развиты навыки проектного управления и командной

работы. В следствие чего их конкурентоспособность на рынке труда повышается. Кроме того, обобщение опыта подобной работы дает педагогу возможность публикации результатов такого опыта.

Кроме причин местного, локального, касающихся конкретной организации, характера стоит выделить влияние грантовой деятельности и на образовательную политику в целом. Успешные грантовые проекты могут стать частью региональных или федеральных программ, основой образовательных стандартов, повлиять на управленческие решения в сфере образования.

Актуальность исследования процесса подготовки педагогических работников к участию в грантовых конкурсах обусловлена необходимостью адаптации общепринятых методов проектного управления к специфике грантовой деятельности в образовании с учетом регионального контекста.

Для оценки эффективности программы проводилась входная и итоговая диагностика. Использовались инструменты LMS Moodle для проведения онлайн-тестирования, анкетирования и сбора обратной связи.

Реализация программы с использованием LMS Moodle позволила эффективно решить ряд проблем:

1. *Проблема целеполагания и постановки задач проекта.* Слушателям было трудно формулировать цели проекта, формулировки зачастую были размытыми, отсутствовала конкретика в формулировании. Поставленные задачи не всегда соответствовали целям, иногда задачи дублировали цель. При этом самое большое затруднение вызвала необходимость сформулировать критерии достижимости цели. С помощью интерактивных заданий в LMS Moodle слушатели отрабатывали навыки формулирования целей по SMART-критериям, декомпозиции целей на задачи и определения показателей достижимости. Использование форумов для peer-to-peer оценки и комментирования работ преподавателем способствовало развитию критического мышления [3].

2. *Проблема описания проблемной ситуации целевой группы.* Данная проблема нашла проявление в неумении (неспособности) автора проекта проанализировать причины возникающих трудностей у представителей целевой группы. Для решения данной проблемы в рамках курса были созданы интерактивные сценарии и кейсы, позволяющие слушателям проводить анализ целевой аудитории, выявлять корневые причины проблем и формулировать их с учетом количественных и качественных данных. Инструменты совместной работы (wiki, семинары) позволяли организовать групповую работу над анализом целевых групп.

3. *Проблема работы с конкурсными документами.* Особое внимание участников грантовых конкурсов должно быть уделено соблюдению структуры заявки. Небрежность на этом этапе приводит к потере баллов при оценке материалов экспертами. Также к ошибкам при работе с конкурсными документами следует отнести технический брак, например, отсутствие копий документов, заверенных электронной подписью, и нарушение сроков подачи документов, что автоматически приводит к отклонению заявки. Для развития навыка работы с формализованными документами в LMS Moodle были размещены шаблоны заявок, инструкции по оформлению и критерии оценки, что позволило слушателям поэтапно отрабатывать навыки подготовки конкурсной документации. Система автоматического тестирования позволяла проводить предварительную проверку заявок на соответствие формальным требованиям.

В рамках программы рассмотрены возможности использования генеративного искусственного интеллекта для формулирования целей и задач проекта для описания проблем целевой группы [4].

Результаты итоговой диагностики показали:

- Уровень понимания грантовых механизмов вырос с 78% до 94%.
- Готовность к участию в грантовых конкурсах увеличилась с 18% до 63%.
- Навыки оформления заявок улучшились на 70% (с 12% до 82%).

Использование LMS Moodle в реализации программы повышения квалификации позволило создать *эффективную образовательную среду*, обеспечивающую:

1. Гибкость и доступность обучения для педагогических работников.
2. Возможность отработки практических навыков через интерактивные задания и симуляции.
3. Систематизацию и структурирование материалов по грантовой деятельности.
4. Организацию обратной связи и поддержки со стороны преподавателей и коллег.
5. Повышение мотивации слушателей за счет использования интерактивных форматов и геймификации [5].

Опыт реализации программы подтвердил целесообразность широкого внедрения LMS Moodle в систему повышения квалификации педагогических работников, особенно в области проектной и грантовой деятельности. Дальнейшие исследования могут быть направлены на разработку и апробацию специализированных плагинов и модулей для LMS Moodle, ориентированных на поддержку грантозаявителей в образовании.

#### СПИСОК ЛИТЕРАТУРЫ

1. Михайлов А.В., Кубаева Т.Н. // Информационные технологии в профессиональной деятельности педагогов дополнительного образования. Мировая наука, 2023. № 6 (75). С. 88-92.
2. Голдина И.И., Зорков В.С. Основные свойства компьютерных технологий в процессе обучения // Образование на современном этапе: тренды, инновации, перспективы. Екатеринбург, 2023. С. 38-39.
3. Рукавишников Е.Е. Разработка интерактивных курсов в системе дополнительного профессионального образования // Известия Волгоградского государственного педагогического университета, 2024. №7 (190). С. 53-64.
4. Литвинов В.Л., Литвинова Е.В. Проблемы и тенденции применения генеративного искусственного интеллекта в образовании // Современное образование: содержание, технологии, качество, 2024. Т. 1. С. 107-109.
5. Балакина Д.С., Голубченко В.А. Перспективы информационных технологий в дополнительном профессиональном образовании // Интеграция информационных технологий в систему профессионального и дополнительного образования. материалы региональной научно-практической конференции. Нижний Новгород, 2023. С. 5-9.

УДК 004.056

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КИБЕРФИЗИЧЕСКИХ СИСТЕМ В ЭПОХУ  
«УМНЫХ ГОРОДОВ»: АКТУАЛЬНЫЕ ПРОБЛЕМЫ РЕГУЛИРОВАНИЯ****Раковский Олег Владимирович, Голакционов Дмитрий Александрович**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича  
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mails: rakovskii.ov@sut.ru, golaktionov@gmail.com

**Аннотация.** Анализ ключевых вызовов в области обеспечения информационной безопасности киберфизических систем (КФС) становится основой критической инфраструктуры современных «умных городов» и цифровых регионов России. Двойственная природа угроз КФС сочетает в себе кибератаки с прямыми физическими последствиями. В работе проводятся исследования пробелов и дублирования в действующей нормативно-правовой базе, регламентирующей данную сферу, и анализируются новые инициативы регуляторов. Особое внимание уделяется вопросам ответственности за инциденты информационной безопасности (ИБ) и необходимости разработки комплексных стандартов, объединяющих требования к программному и аппаратному обеспечению. При решении актуальной проблемы рассматриваются рекомендации по совершенствованию государственной политики и системы подготовки кадров для опережающего противодействия угрозам безопасности КФС.

**Ключевые слова:** киберфизические системы; «умные города»; кибератаки; информационная безопасность; IIoT; human-on-the-loop.

**INFORMATION SECURITY OF CYBER-PHYSICAL SYSTEMS IN THE «SMART CITY»  
ERA: CURRENT REGULATORY CHALLENGES****Rakovskiy Oleg, Golaktionov Dmitry**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications,  
22 Bolshhevikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mails: rakovskii.ov@sut.ru, golaktionov@gmail.com

**Abstract.** Analysis of the key challenges in ensuring the information security of cyber-physical systems (CPS) is fundamental to the critical infrastructure of modern «smart cities» and digital regions in Russia. The dual nature of CPS threats combines cyberattacks with direct physical consequences. This study investigates gaps and redundancies within the current regulatory and legal framework governing this domain and analyzes new initiatives proposed by regulators. Particular attention is paid to the issues of liability for information security (IS) incidents and the necessity of developing comprehensive standards that integrate requirements for both software and hardware. In addressing this pertinent problem, the paper proposes recommendations for improving state policy and the system of professional training to enable proactive countermeasures against CPS security threats.

**Keywords:** cyber-physical systems; smart cities; cyberattacks; information security; IIoT; human-on-the-loop.

Стремительная цифровая трансформация экономики и социальной сферы России немыслима без внедрения киберфизических систем (КФС). Эти технологии, интегрирующие вычислительные ресурсы с физическими процессами, лежат в основе «умных» систем ЖКХ, автономного транспорта, интеллектуальных энергосетей, телемедицины и промышленного Интернета вещей (IIoT). Их повсеместное распространение создает принципиально новый ландшафт угроз информационной безопасности, где успешная кибератака перестает быть виртуальным инцидентом и превращается в событие с катастрофическими физическими последствиями. Актуальность вопроса заключается в поиске баланса между стимулированием инноваций и обеспечением надежной защиты, что требует адекватного и опережающего государственного регулирования.

Уникальность КФС заключается в стирании границы между киберпространством и реальным миром. Если традиционная атака на сервер приводит к утечке данных или простою сервиса, то атака на КФС способна привести к последствиям:

- физические разрушения: вмешательство в систему управления промышленным роботом или станком с ЧПУ;
- техногенные катастрофы: взлом SCADA-системы энергосетей или водоснабжения;
- транспортные коллапсы: перехват управления беспилотным автомобилем или нарушение работы светофорной сети «умного города»;
- вред здоровью: кибератака на подключенный кардиостимулятор или систему дистанционного мониторинга пациента.

Этот переход от конфиденциальности к безопасности human-on-the-loop делает задачу обеспечения ИБ КФС задачей национальной безопасности.

Действующее российское законодательство в области ИБ (прежде всего, Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ»), в основном сфокусировано на информационных системах и автоматизированных системах управления технологическим процессом (АСУ ТП). Киберфизические системы, как более сложные и распределенные гибридные системы, часто попадают под регулирование сразу нескольких отраслей права, что создает правовые коллизии и зоны безответственности:

1. Дублирование и противоречия: требования к одному и тому же компоненту КФС (например, к «умному» счетчику) могут регулироваться разными ведомствами (ФСТЭК, ФСБ, Роскомнадзор, отраслевые министерства), чьи нормативные акты не всегда синхронизированы;

2. Отсутствие комплексных стандартов: существующие стандарты (серии ГОСТ Р МЭК 62443) касаются в основном промышленных систем. Для гражданского сектора (IoT-устройства, умный дом, телемедицина) требования разрознены или носят рекомендательный характер, что создает риски из-за использования уязвимого «железа» и ПО.

3. Вопрос ответственности: в случае инцидента с беспилотным автомобилем сложно определить виновного (производитель программного обеспечения, разработчик сенсоров, телеком-оператор, обеспечивающий связь, владелец, не установивший обновление безопасности) при распределении вины в случае инцидентов. Это приводит к ситуации, когда технологическая сложность системы превышает разрешающую способность существующих правовых институтов, требующих модернизации.

Государство осознает эти вызовы и в рамках реализации стратегии развития информационного общества и национальных проектов («Цифровая экономика», «Безопасные качественные дороги») предпринимаются шаги по формированию новой регуляторной среды:

- разработка отраслевых требований: активно ведутся работы по созданию профильных стандартов ИБ для беспилотного транспорта, интеллектуальных энергосистем, телемедицинского оборудования;

- сертификация и паспортизация: ужесточаются требования к сертификации импортного оборудования и ПО для КФС, рассматриваются модели обязательной паспортизации с указанием уязвимостей и их жизненного цикла;

- стимулирование отечественных решений: поддержка разработки российских компонентов для КФС (микроэлектроника, ОС, средства криптозащиты) рассматривается как ключевой элемент обеспечения суверенитета и безопасности.

Никакие законы не работают без квалифицированных специалистов. Традиционные программы по информационной безопасности должны быть пересмотрены с учетом специфики КФС. Существует острая необходимость в подготовке киберфизических security-инженеров, которые понимают не только сетевые протоколы и криптографию, но и основы мехатроники, теории управления и физических процессов.

Обеспечение информационной безопасности киберфизических систем является комплексной междисциплинарной проблемой, требующей консолидированных усилий государства, бизнеса и научного сообщества. Необходима скорейшая разработка целостной и непротиворечивой нормативной базы, устанавливающей четкие «правила игры» для всех участников рынка. Важнейшим элементом этой политики должно стать опережающее развитие отечественных технологий и подготовка кадров, способных не только реагировать на инциденты, но и проектировать безопасные и устойчивые системы с самого начала. Успех в этом направлении станет залогом не только технологического суверенитета, но и физической безопасности граждан России в цифровую эпоху.

#### СПИСОК ЛИТЕРАТУРЫ

1. Аррыкова Г. К., Мурадов Э. Ч., Назаров Д. С., Реджепмырадов Г. Р. Кибербезопасность умных городов: вызовы цифровизации инфраструктуры // Наука и мировоззрение. 2025. № 33 [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/kiberbezopasnost-umnyh-gorodov-vyzovy-tsifrovizatsii-infrastruktury> (дата обращения: 26.08.2025).
2. Курчеева Г.И., Денисов В.В. Угрозы для информационной безопасности в высокоорганизованных системах типа «Умный город» // Интернет-журнал «Наукоедение» Т. 8, № 3, 2016. URL: <http://naukovedenie.ru/PDF/146EVN316.pdf> (доступ свободный).
3. Security Challenges and Solutions in Smart Cities. [Электронный ресурс]. URL: [https://www.researchgate.net/publication/377402349\\_Security\\_Challenges\\_and\\_Solutions\\_in\\_Smart\\_Cities](https://www.researchgate.net/publication/377402349_Security_Challenges_and_Solutions_in_Smart_Cities) (дата обращения: 26.08.2025).

УДК 004.057.8

#### ОЦЕНКА ТОЧНОСТИ RSSI-МЕТОДОВ ДЛЯ ПОЗИЦИОНИРОВАНИЯ WI-FI УСТРОЙСТВ

**Синицына Ольга Александровна, Ковзур Максим Михайлович, Дрепа Владислав Евгеньевич**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

e-mails: [olga.sinicina.02@mail.ru](mailto:olga.sinicina.02@mail.ru), [maxkovzur@mail.ru](mailto:maxkovzur@mail.ru), [drepa.ve@sut.ru](mailto:drepa.ve@sut.ru)

**Аннотация.** Рассматривается алгоритм позиционирования Wi-Fi устройств на основе измерений мощности принимаемого сигнала (RSSI). Предложенный метод включает модифицированную модель затухания сигнала в свободном пространстве и оптимизацию параметров с использованием алгоритма L-BFGS-B для минимизации ошибки локализации. Проведённые испытания демонстрируют достижение точности определения местоположения в диапазоне 1–3 метров в условиях типичных помещений.

**Ключевые слова:** беспроводные сети; локализация точек доступа; RSSI; оптимизация; модель затухания сигнала.

#### RSSI-BASED LOCALIZATION ACCURACY FOR WIRELESS DEVICES

**Sinitsyna Olga, Kovzur Maxim, Drepa Vladislav**

The Bonch-Bruевич Saint Petersburg State University of Telecommunications

22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia

e-mails: [olga.sinicina.02@mail.ru](mailto:olga.sinicina.02@mail.ru), [maxkovzur@mail.ru](mailto:maxkovzur@mail.ru), [drepa.ve@sut.ru](mailto:drepa.ve@sut.ru)

**Abstract.** The study examines a Wi-Fi device positioning algorithm based on received signal strength indicator (RSSI) measurements. The proposed method incorporates a modified free-space path loss model and utilizes the L-BFGS-B optimization algorithm to minimize localization errors. Experimental results demonstrate positioning accuracy within 1–3 meters in typical indoor environments.

**Keywords:** wireless networks; access point localization; RSSI; optimization; signal attenuation model.

Современные беспроводные сети требуют точного определения местоположения точек доступа (ТД) [1-2] для обеспечения стабильного покрытия и выявления несанкционированных устройств. Традиционные методы, такие как триангуляция или fingerprinting, часто требуют значительных вычислительных ресурсов или сложной инфраструктуры. В отличие от них, предложенный метод использует доступные измерения RSSI и адаптивную модель затухания сигнала, что значительно снижает затраты на внедрение.

Основные этапы метода включают:

1. Сбор данных: измерение RSSI в различных точках помещения с фиксацией координат.
2. Предварительную обработку: фильтрацию зашумленных сигналов и нормализацию данных.
3. Оптимизацию: применение алгоритма L-BFGS-B [3] для минимизации функции ошибки, учитывающей расхождения между расчетными и фактическими расстояниями до ТД.

Ключевым преимуществом метода является использование взвешенной квадратичной ошибки, которая уменьшает влияние слабых сигналов на итоговый результат. Кроме того, коэффициент затухания в модели динамически корректируется в зависимости от типа помещения (офис, жилое здание, открытое пространство), что повышает точность расчетов.

Тестирование метода проводилось в помещении размером 10×9 метров с четырьмя точками измерений. Средняя погрешность локализации составила 1,2 метра при времени расчета менее 5 секунд на стандартном ПК.

Перспективы развития метода включают:

- интеграцию с системами автоматизированного проектирования сетей;
- разработку механизмов автоматической настройки параметров модели на основе машинного обучения.

Таким образом, предложенный метод предлагает решение для задач локализации ТД, сочетающее высокую точность с низкими требованиями к ресурсам [4]. Его внедрение может упростить процессы развертывания и обслуживания Wi-Fi [5, 6] сетей в различных условиях.

#### СПИСОК ЛИТЕРАТУРЫ

1. Дрепа В. Е., Киструга А. Ю., Ковцур М. М. Точность определения местоположения Wi-Fi клиента в свободном пространстве при использовании индикатора уровня принимаемого сигнала // Региональная информатика (РИ-2022) : материалы юбилейной XVIII Санкт-Петербургской междунар. конф. Санкт-Петербург, 2022. С. 549–550.
2. Петрова Т. В. Определение способов обнаружения нелегитимной точки доступа в проводной сети организации / Т. В. Петрова, М. М. Ковцур, П. В. Карельский, А. В. Поляничева // Региональная информатика и информационная безопасность : материалы Юбилейной XVIII Санкт-Петербургской международной конференции (РИ-2022). Санкт-Петербург, 2022. С. 612–617.
3. Метод BFGS или один из самых эффективных методов оптимизации. Пример реализации на Python [Электронный ресурс] URL: <https://habr.com/ru/articles/333356/> (дата обращения: 06.07.2025).
4. Махмутова Н. Ф., Ковцур М. М., Петрова Т. В., Киструга А. Ю. Исследование подходов оценки и повышения производительности беспроводной сети // Региональная информатика и информационная безопасность : сб. тр. Санкт-Петербургской междунар. конф. Санкт-Петербург, 2023. С. 389–393.
5. IEEE 802.11-2020: Wireless LAN Standards // IEEE Xplore [Электронный ресурс]. URL: <https://ieeexplore.ieee.org/document/9363693> (дата обращения: 08.07.2025).
6. Rappaport T.S. Wireless Communications: Principles and Practice. 2nd ed. Prentice Hall, 2002. 707 p.

УДК 004.056

#### АНАЛИЗ ПРИМЕНИМОСТИ МЕТОДОВ МОДИФИКАЦИИ БАЙТ-КОДА ДЛЯ ВЛОЖЕНИЯ ЦИФРОВОГО ВОДЯНОГО ЗНАКА В SCALA-ПРОГРАММЫ

Соколов Игорь Всеволодович

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mail: isokol0303@gmail.com

**Аннотация.** Рассматривается метод внедрения цифрового водяного знака в программы, разработанные на языке Scala, посредством модификации байт-кода. Определены устойчивые точки вставки, обеспечивающие сохранность водяного знака после обфускации и декомпиляции при сохранении корректности работы программ.

**Ключевые слова:** защита программного обеспечения; цифровой водяной знак; Scala; байт-код; JVM; Apache BCEL.

#### ANALYSIS OF THE APPLICABILITY OF BYTECODE MODIFICATION METHODS FOR EMBEDDING A DIGITAL WATERMARK IN SCALA PROGRAMS

Sokolov Igor

The Bonch-Bruevich Saint Petersburg State University of Telecommunications  
22 Bolshhevikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mail: isokol0303@gmail.com



**Abstract.** A method for embedding a digital watermark into programs developed in Scala via bytecode modification is considered. Stable insertion points are identified that ensure the watermark remains intact after obfuscation and decompilation while preserving correct program execution.

**Keywords:** software protection; digital watermark; Scala; bytecode; JVM; Apache BCEL.

В условиях масштабного распространения и несанкционированного копирования программного обеспечения задача защиты авторских прав приобретает ключевое значение. Одним из перспективных направлений является внедрение цифровых водяных знаков на уровне байт-кода. Несмотря на наличие апробированных подходов для Java, их перенос на язык Scala сопряжен с рядом особенностей, обусловленных сложной структурой генерируемых компилятором .class-файлов [1–3].

Целью исследования являлась оценка применимости существующих методик модификации байт-кода для вложения цифрового водяного знака в программы на языке Scala. Для достижения цели был проведен анализ структуры скомпилированных модулей, включающих различные языковые конструкции: функции высшего порядка, замыкания, трейты и компаньон-объекты. Исследование выполнялось с применением библиотеки Apache BCEL, позволяющей осуществлять прямую работу с байт-кодом без декомпиляции исходного кода [4–6].

Анализ показал, что компилятор Scala формирует дополнительный набор служебных классов и методов, отсутствующих в аналогичных Java-программах, что существенно влияет на стратегию поиска устойчивых точек внедрения. Наиболее перспективными для модификации признаны условные переходы (if\_icmpge, if\_icmpreq, goto) и последовательность загрузки констант (ldc), допускающие эквивалентные трансформации без изменения семантики работы программы [5–8].

Экспериментально подтверждено, что модификация выбранных участков байт-кода позволяет встроить цифровой водяной знак, сохраняющийся после операций обфускации и декомпиляции. Результаты демонстрируют применимость подхода для защиты Scala-программ с минимальным влиянием на производительность и размер исполняемых файлов [9–12].

Таким образом, использование методов модификации байт-кода в сочетании с особенностями трансляции Scala открывает перспективы для разработки автоматизированных инструментов внедрения и устойчивости цифровых водяных знаков в JVM-совместимых языках.

#### СПИСОК ЛИТЕРАТУРЫ

1. Hamilton J., Danicic S. An Evaluation of Static Java Bytecode Watermarking. 2010. [Электронный ресурс]. URL: <https://jameshamilton.eu/sites/default/files/JavaBytecodeWatermarkingSurvey.pdf> (дата обращения: 11.08.2025).
2. Akbar Z. Watermarking Java Programs using Dummy Methods with Dynamically Opaque Predicates. 2010. [Электронный ресурс]. URL: [https://www.researchgate.net/publication/45912770\\_Watermarking\\_Java\\_Programs\\_using\\_Dummy\\_Methods\\_with\\_Dynamically\\_Opaque\\_Predicates](https://www.researchgate.net/publication/45912770_Watermarking_Java_Programs_using_Dummy_Methods_with_Dynamically_Opaque_Predicates) (дата обращения: 11.08.2025).
3. Изучаем Scala. [Электронный ресурс]. URL: <https://docs.scala-lang.org> (дата обращения: 30.06.2025).
4. Paganoni M., Furia C. A. Furia reasoning about exceptional behavior at the level of java bytecode. September, 2024.
5. Hamilton J. The Problems with the execution path watermark algorithm for java bytecode // International Journal of Security and Its Applications, 2024. № 10 (7). Pp. 147-156.
6. Шариков П. И., Красов А. В., Штеренберг С. И. Методика создания и вложения цифрового водяного знака в исполняемые java файлы на основе замен опкодов // Т-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 3. С. 66-70.
7. Шариков П. И. Исследование атаки обфускацией на байт-код java-приложения с целью разрушения или повреждения цифрового водяного знака // I-methods. 2022. Т. 14. № 1. EDN GQGKIV.
8. Шариков П. И., Красов А. В. Исследование возможности использования java-агентов для вложения скрытого цифрового водяного знака непосредственно перед запуском java-приложения // Вестник СПбГУПТД. Серия I Естеств. и технич. науки. 2019. № 4. С. 14-18. EDN QQUVYX.
9. Шариков П. И. Методика обфускации байт-кода Java-приложения с целью его защиты от атак декомпиляцией // Вестник СПбГУПТД. Серия I Естественные и технические науки. 2022. № 1. С. 64-72. DOI 10.46418/2079-8199\_2022\_1\_10. EDN AUOFNA.
10. Шариков П. И., Цветков А. Ю., Сигачева В. В., Сиротина Л. К. Исследование и алгоритм предотвращения эксплуатации уязвимостей библиотеки журналирования Log4j в информационных системах Java-приложений // Вестник СПбГУПТД. Серия I. Естественные и технические науки. 2023. № 4. С. 100-106. DOI 10.46418/2079-8199\_2023\_4\_19. EDN BULSON.
11. Шариков П. И. Методика создания и скрытого вложения цифрового водяного знака в байт-код class-файла на основе не декларированных возможностей виртуальной машины java // Современная наука: актуальные проблемы теории и практики. Серия. Естественные и технические науки. 2023. № 7-2. С. 165-174. DOI 10.37882/2223-2982.2023.7-2.37. — EDN YBEWYQ.
12. Дудников И. А., Шариков П. И., Майоров А. В. Методика анализа журналов событий информационных систем с использованием Elasticsearch для обнаружения сигналов о вредоносных действиях в информационной системе // Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. 2025. № 1. С. 120-134. DOI 10.61260/2218-130X-2025-1. EDN ZQCEXG.



## МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА «БЕЗОПАСНЫЕ СИСТЕМЫ СВЯЗИ»

УДК 004.056

### ТРУДНОСТИ ПЕРЕХОДА НА СЕТИ СВЯЗИ НОВОГО ПОКОЛЕНИЯ

Аветиков Артем Анатольевич<sup>2</sup>, Задбоев Вадим Александрович<sup>1</sup>, Тимофеев Артём Михайлович<sup>2</sup>

<sup>1</sup> Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

<sup>2</sup> Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Большевикова пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

e-mails: artemmt97@mail.ru, avetikov.aa@sut.ru, zadboev89@mail.ru

**Аннотация.** Несмотря на все новые возможности, переход от 5G к 6G сопровождается ростом киберугроз. Сети 5G сталкиваются с уязвимостями IoT, сетевого срезания и атаками на технологии радиодоступа. В 6G эти риски усиливаются из-за высокой плотности устройств, интеграции не наземных сетей, угроз ИИ и отсутствия квантово-устойчивого шифрования. Угрозы приобретают системный характер, требуя масштабируемых решений. Для защиты предлагается внедрение Zero-Trust, сквозного шифрования, блокчейна и постквантовой криптографии, а также активное межотраслевое сотрудничество.

**Ключевые слова:** уязвимости; сети 5G; сети 6G; Zero Trust; кибербезопасность; криптография.

### DIFFICULTIES OF TRANSITION TO NEW GENERATION COMMUNICATION NETWORKS

Avetikov Artem<sup>2</sup>, Zadboev Vadim<sup>1</sup>, Timofeev Artyom<sup>2</sup>

<sup>1</sup> The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

<sup>2</sup> The Bonch-Bruевич Saint Petersburg State University of Telecommunications

22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia

e-mails: artemmt97@mail.ru, avetikov.aa@sut.ru, zadboev89@mail.ru

**Abstract.** Despite all the new opportunities, the transition from 5G to 6G is accompanied by an increase in cyber threats. 5G networks face vulnerabilities from IoT, network slicing, and attacks on radio access technologies. In 6G, these risks are amplified by high device density, non-terrestrial network integration, AI threats, and the lack of quantum-resistant encryption. Threats are becoming systemic, requiring scalable solutions. To protect against this, the implementation of Zero-Trust, end-to-end encryption, blockchain, and post-quantum cryptography, as well as active cross-industry cooperation, are proposed.

**Keywords:** vulnerabilities; 5G networks; 6G networks; Zero Trust; cybersecurity; cryptography.

Развитие мобильных сетей связи от пятого к шестому поколению знаменует собой переход к принципиально новой цифровой экосистеме, где высокая скорость, сверхнизкие задержки и масштабная интеграция с интеллектуальными технологиями становятся основой для трансформации транспорта, здравоохранения, промышленности и городской инфраструктуры.

Вместе с тем, усложнение архитектуры сетей, рост числа подключённых устройств и активное использование искусственного интеллекта и виртуализации открывают широкие возможности для кибератак.

Сети 6G, несмотря на технологические прорывы, наследуют и усугубляют уязвимости 5G, одновременно сталкиваясь с принципиально новыми вызовами. Если в 5G основные угрозы связаны с незащищёнными IoT-устройствами, которые становятся точками входа для масштабных атак, то в 6G эта проблема усугубляется экстремальной плотностью подключённых устройств, что делает управление идентификацией и доступом чрезвычайно сложным.

Архитектура 6G предполагает миллиарды датчиков и устройств в умных городах, медицине и промышленности, что увеличивает поверхность атаки и требует новых подходов к аутентификации и шифрованию на уровне каждого узла [1–2].

Технология сетевого срезания, уже используемая в 5G, в 6G становится ещё более критичной: виртуальные срезы будут обслуживать разнородные приложения — от автономного транспорта до телемедицины. Уязвимость одного среза может быть использована для перехода в другие, что требует строгой изоляции и динамического мониторинга. В 6G эта изоляция должна быть не только программной,

но и криптографически обеспеченной, с применением механизмов сквозного шифрования и микросегментации [3].

Интеграция не наземных сетей (NTN), включая спутники и высотные платформы, добавляет сложности в управление handover-процедурами и аутентификацией. Переключения между наземными и спутниковыми сегментами происходят чаще и менее предсказуемо, что создаёт окна для подмены базовых станций, перехвата данных и DoS-атак. Отсутствие единой модели доверия между различными сетевыми доменами требует построения децентрализованных систем управления идентификацией, например, на основе блокчейна.

Искусственный интеллект, играющий центральную роль в 6G для оптимизации трафика, управления ресурсами и обнаружения аномалий, сам становится объектом атак.

Такие угрозы, как инверсия модели, извлечение обучающих данных и отравление данных, могут привести к компрометации всей системы безопасности. Особенно опасны атаки, направленные на подмену решений ИИ, что может привести к перенаправлению трафика, сбоям в работе критической инфраструктуры или утечке конфиденциальной информации [4–5].

Одной из фундаментальных проблем 6G является отсутствие квантово-устойчивой криптографии. Современные алгоритмы шифрования, такие как RSA и ECC, будут уязвимы перед квантовыми компьютерами. Поскольку 6G-сети будут функционировать десятилетиями, их необходимо проектировать с учётом будущих квантовых угроз.

Уже сейчас требуется переход к постквантовым криптографическим стандартам, которые обеспечат долгосрочную защиту данных [6].

Архитектура безопасности 6G должна строиться по принципу Zero Trust — ни один узел не считается доверенным по умолчанию. Это включает постоянную верификацию устройств, динамическое управление доступом, мониторинг поведения и автоматическое реагирование на аномалии.

Такой подход особенно важен в условиях гетерогенной среды, где взаимодействуют наземные, воздушные и космические сегменты [7–8].

Безопасность 6G невозможно обеспечить в изоляции. Необходима координация между операторами связи, производителями оборудования, разработчиками ИИ, научными институтами и регуляторами. Только совместная работа позволит выработать единые стандарты, протестировать новые решения и оперативно реагировать на появление новых угроз [9].

В отличие от 5G, где безопасность часто добавлялась как дополнение, в 6G она должна быть заложена в основу с самого начала — по принципу «безопасность по проекту» (security by design). Это означает, что все компоненты сети, от физического уровня до прикладных сервисов, должны разрабатываться с учётом потенциальных угроз и возможностей защиты.

Таким образом, безопасность 6G — это не просто улучшенная версия защиты 5G, а качественно новый подход, требующий системного мышления, междисциплинарных решений и долгосрочного планирования.

Успешное внедрение 6G будет зависеть не столько от скорости передачи данных, сколько от способности сети противостоять сложным и динамичным киберугрозам будущего.

#### СПИСОК ЛИТЕРАТУРЫ

1. Лемешко, Д. В. Безопасность ИОТ-устройств, подключенных к сетям пятого и шестого поколений / Д. В. Лемешко // Информационные технологии в науке, бизнесе и образовании. Проблемы обеспечения цифрового суверенитета государства : Материалы XIII Межд. научно-практ. Конф. студентов, аспирантов и молодых ученых, Москва, 26 ноября 2021 г. / Под общ. Ред. А.М. Прохорова, А.В. Царегородцева. М. : Московский государственный лингвистический университет, 2022. С. 45-48. EDN YRHDVV.
2. Белова, М. А. Безопасность сетей 5G / М. А. Белова, В. И. Рыськина // Региональная информатика и информационная безопасность : Сборник трудов конференций: Санкт-Петербургской междунар. Конф. и Санкт-Петербургской межрегиональной конференции, Санкт-Петербург, 28–30 ноября 2020 года. Вып. 8. СПб. : Региональная общественная организация СПОИСУ, 2020. С. 256-261. EDN LTWTGD.
3. Калинина, А. И. Уязвимости протоколов сетей 5G / А. И. Калинина // Интернаука. 2019. № 43-1(125). С. 14-17. EDN IQMQVB.
4. Южаков, А. В. Информационная безопасность мобильной связи 6G в России / А. В. Южаков, В. И. Соловьев // Цифровые системы и модели: теория и практика проектирования, разработки и применения : Материалы национальной (с международным участием) научно-практической конференции, Казань, 10–11 апреля 2024 года. Казань: Казанский государственный энергетический университет, 2024. С. 1415-1418. EDN RLYNWW.
5. Кучерявый, Е. А. Анализ информационной безопасности на техническую спецификацию Network 2030 Architecture Framework для 6G сетей / Е. А. Кучерявый, И. А. Смирнов // Актуальные аспекты развития науки и общества в эпоху цифровой трансформации : Сборник материалов XI Международной научно-практической конференции, Москва, 06 ноября 2023 года. Москва: ООО «Издательство АЛЕФ», 2023. С. 54-63. DOI 10.34755/IROK.2023.96.12.189. EDN NNDNFE.
6. Липатников В.А., Шевченко А.А. Проактивное управление информационной безопасностью автоматизированной системы радиоконтроля // Информационные системы и технологии. 2019. № 4(114). С. 112-121.
7. Липатников В.А., Ложечкин А.А., Шевченко А.А. Построение комплексной защиты киберфизической системы от деструктивных воздействий // Информационные системы и технологии. 2020. № 6(122). С. 112-120.
8. Липатников В.А., Шевченко А.А. Модель процесса управления информационной безопасностью распределенной информационной системы на основе выявления и оценки уязвимостей // Информационные системы и технологии. 2018. № 1(105). С. 114-123.
9. Задбоев, В. А. анализ возможностей отечественных средств, применяемых для мониторинга информационной безопасности сетей передачи данных / В. А. Задбоев, Н. А. Роговой, А. А. Шевченко // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2024) : Материалы XIII Международной научно-технической и научно-методической конференции, Санкт-Петербург, 27–28 февраля 2024 года. СПб: СПбГУ телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2024. С. 308-313. EDN DQGVDS.

УДК 004.932.2

**ОЦЕНКА ЭФФЕКТИВНОСТИ СИСТЕМЫ АВТОМАТИЗИРОВАННОГО АНАЛИЗА  
ОКТ ИЗОБРАЖЕНИЙ****Аксенова Любовь Евгеньевна**

ООО «Пространство интеллектуальных решений»

Адмирала Серебрякова наб., 49, Новороссийск, 353905, Россия

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича,

Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

Новороссийский политехнический институт (филиал) ФГБОУ ВПО «КубГТУ»

Карла Маркса ул., 20, Новороссийск, 353900, Россия

e-mail: axenovalubov@gmail.com

**Аннотация.** Оптическая когерентная томография (ОКТ) является ключевым методом диагностики офтальмопатологий, однако её интерпретация требует значительных временных затрат. В работе проведена оценка эффективности автоматизированной системы анализа ОКТ-изображений, основанной на глубоких нейронных сетях. Сравнение показало, что алгоритм выполняет измерение количественных метрик и анализ изображений в 16-18 раз быстрее эксперта и в 50-60 раз быстрее начинающего врача, обеспечивая стандартизированные результаты и снижая вариабельность между разным специалистами. Система демонстрирует высокий потенциал для повышения доступности офтальмологической помощи, особенно для начинающих врачей и в условиях телемедицинских консультаций.

**Ключевые слова:** ОКТ; искусственный интеллект; сегментация; офтальмология; телемедицина.

**EVALUATION OF THE EFFECTIVENESS OF AN AUTOMATED OCT IMAGE ANALYSIS SYSTEM****Aksenova Lyubov**

Predict Space LLC

49Admiral Serebryakova Emb, Novorossiysk, 353905, Russia

The Bonch-Bruevich Saint Petersburg State University of Telecommunications,

22 Bolshevnikov Av, bldg 1, St. Petersburg, 193232, Russia

Novorossiysk Polytechnic Institute (branch) of the Kuban State Technological University

20 Karl Marx St, Novorossiysk, 353900, Russia

e-mail: axenovalubov@gmail.com

**Abstract.** Optical coherence tomography (OCT) is a key method for diagnosing ophthalmic pathologies; however, its interpretation requires significant time costs. This study evaluated the effectiveness of an automated OCT image analysis system based on deep neural networks. The comparison showed that the algorithm performs quantitative metric measurements and image analysis 16–18 times faster than an inexperienced physician and 50–60 times faster than an expert, providing standardized results and reducing inter-observer variability. The system demonstrates high potential for improving the accessibility of ophthalmologic care, especially for novice doctors and in the context of telemedicine consultations.

**Keywords:** OCT; artificial intelligence; segmentation; ophthalmology; telemedicine.

Оптическая когерентная томография (ОКТ) является «золотым стандартом» визуализации структур сетчатки и позволяет выявлять широкий спектр офтальмопатологий на ранних стадиях [1, 2]. Однако интерпретация данных остаётся трудоёмким процессом. Автоматизация анализа изображений с использованием технологий искусственного интеллекта открывает перспективы ускорения диагностики, снижения межнаблюдательной вариабельности и внедрения телемедицинского мониторинга [3, 4]. Целью настоящей работы являлось измерение эффективности применения автоматизированной системы анализа изображений ОКТ в клинической практике врача офтальмолога.

В работе использована автоматизированная система анализа изображений ОКТ, которая основана на архитектуре глубоких сверточных нейронных сетей, обученных на многоцентровых наборах данных (OCTDL, OCTID, OCT2017) с таких ОКТ приборов как Heidelberg, Zeiss, Optovue [6,7]. Дополнительно реализован модуль сегментации на базе U-Net для детекции и количественной оценки биомаркеров — отслойки пигментного эпителия (PED), субретинальной (SRF) и интравитреальной жидкости (IRF) [6]. Пилотное внедрение проведено на выборке пациентов с н-ВМД, проходивших anti-VEGF терапию. Врачебные замеры количественных параметров (высота, протяжённость PED и др.) сопоставлялись с результатами алгоритма.

В исследовании проводилось сравнение временных затрат врача-эксперта, начинающего врача и автоматизированного алгоритма при выполнении двух типов задач:

Измерение метрик — ручное определение количественных параметров (протяжённость и высота структур) с использованием встроенной в программное обеспечение прибора линейки.

Анализ ОКТ — просмотр томограмм, оценка наличия патологических структур (PED, SRF, IRF и др.) и формулировка заключения о наличии заболеваний. Для оценки производительности были проанализированы 30 изображений ОКТ. Время выполнения задач фиксировалось для каждого участника с помощью секундомера.

Алгоритм проводил автоматизированный анализ всего изображения с выводом типа заболевания и наличия биомаркеров, а также расчёт числовых характеристик биомаркеров.

Среднее время измерения количественных метрик составило 14,1 с у эксперта, 48,7 с у начинающего врача и 0,8 с у алгоритма. При сопоставлении видно, что алгоритм выполняет задачу приблизительно в 18 раз быстрее эксперта и в 60 раз быстрее начинающего специалиста. Время анализа изображений составило 32,4 с у эксперта, 101,7 с у врача и 2 с у алгоритма, что соответствует ускорению примерно в 16 раз по сравнению с экспертом и в 50 раз по сравнению с начинающим врачом. Автоматическая сегментация формирует готовые количественные показатели (площадь, высота, протяжённость PED, SRF, IRF), минимизируя вероятность ошибок ручного ввода. Важным преимуществом является снижение межнаблюдательной вариабельности: при одинаковых изображениях значения, полученные врачами разного уровня подготовки, могут различаться, тогда как алгоритм обеспечивает стандартизированные и воспроизводимые результаты. Так же можно отметить, что за счет сокращения времени анализа может быть получен и экономический эффект внедрения такой системы благодаря увеличению потока пациентов и возможностей телемедицинского мониторинга в удалённых регионах.

Наибольший практический эффект от внедрения автоматизированной системы наблюдается у специалистов с ограниченным опытом работы. Внедрение таких алгоритмов в клиническую практику может обеспечить ускорение диагностики и снижение нагрузки на офтальмологов; повышение доступности офтальмологической помощи в условиях ограниченных ресурсов; расширение охвата скрининговыми программами и выявляемости заболеваний на ранних стадиях; формирование базы для динамического мониторинга и прогнозирования исходов терапии.

#### СПИСОК ЛИТЕРАТУРЫ

1. Christoph R, Nicole C. Retinal pigment epithelium tears: risk factors, mechanism and therapeutic monitoring. *Ophthalmologica*. 2016;235: 1–9. doi: .10.1159/000439445.
2. Будзинская М.В., Шеланкова А.В. Разрывы ретинального пигментного эпителия при возрастной макулярной дегенерации. *Вестник офтальмологии*. 2021;137(3): 115–120.
3. Schmidt-Erfurth U, Vogl W, Jampol LM, Bogunović H. Application of Automated Quantification of Fluid Volumes to Anti-VEGF Therapy of Neovascular Age-Related Macular Degeneration. *Ophthalmology*. 2020; 127(9): 1211–1219. doi: 10.1016/j.ophtha.2020.03.010.
4. Rohm M, Tresp V, Müller M, Kern C, Manakov I, Weiss M, Sim DA, Priglinger S, Keane PA, Kortuem K. Predicting Visual Acuity by Using Machine Learning in Patients Treated for Neovascular Age-Related Macular Degeneration. *Ophthalmology*. 2018 Jul;125(7):1028–1036. doi: 10.1016/j.ophtha.2017.12.034.
5. Schlegl T, Waldstein SM, Bogunovic H, Endstraßer F, Sadeghipour A, Philip A, et al. Fully Automated Detection and Quantification of Macular Fluid in OCT Using Deep Learning. *Ophthalmology*. 2018; 125(4): 549–558. doi: 10.1016/j.ophtha.2017.10.031.
6. Aksenova L.E., Aksenov K.D., Kozina E.V., Myasnikova V.V. AUTOMATED SYSTEM FOR ANALYSIS OF OCT RETINA IMAGES DEVELOPMENT AND TESTING // *Doklady Mathematics*. 2023. T. 108. № S2. C. S310–S316.
7. L.E. Aksenova, K.D. Aksenov, A.V. Prisyazhnyuk, V.V. Myasnikova, A.V. Krasov. Development of an OCT data classification model for determining the presence and type of ophthalmic diseases. *Computing, Telecommunication and Control*. 2024, Vol. 17, No. 3, Pp. 103–113. DOI: 10.18721/JCSTCS.17310.

УДК 004.056.5

#### ФРАГМЕНТАРНОСТЬ ДАННЫХ ОБ УЯЗВИМОСТЯХ КАК ВЫЗОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПУТИ ЕГО ПРЕОДОЛЕНИЯ

Антипина Софья Олеговна, Пестов Игорь Евгеньевич

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

Большевиков пр., 22, корп.1, Санкт-Петербург, 193232, Россия

e-mails: sofyaantipinaa@yandex.ru, pestov.ie@sut.ru

**Аннотация.** Современные информационные системы функционируют в условиях стремительного роста числа уязвимостей в программном и аппаратном обеспечении. Сведения о них распределены между множеством международных и национальных баз данных, что приводит к фрагментарности информации и снижает её практическую ценность для специалистов. В докладе рассматривается актуальность создания единого ресурса, способного централизовать сведения об уязвимостях и обеспечить их эффективное использование. Подчёркивается, что централизация данных повышает полноту картины угроз, сокращает время реагирования на инциденты и способствует формированию устойчивых цифровых инфраструктур, способных противостоять растущему числу кибератак.

**Ключевые слова:** уязвимость; информационная безопасность; база данных; централизация; интеграция; фрагментарность; реагирование на угрозы.

#### FRAGMENTATION OF VULNERABILITY DATA AS A CHALLENGE TO INFORMATION SECURITY AND WAYS TO OVERCOME IT

Antipina Sofya, Pestov Igor

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia

e-mails: sofyaantipinaa@yandex.ru, pestov.ie@sut.ru

**Abstract.** Modern information systems operate under conditions of a rapid increase in the number of vulnerabilities in software and hardware. Information about them is distributed across numerous international and national databases, which leads to fragmentation and reduces its practical value for specialists. The report examines the relevance

of creating a unified resource capable of centralizing vulnerability data and ensuring its effective use. It is emphasized that data centralization improves the completeness of the threat landscape, reduces incident response time, and contributes to the formation of resilient digital infrastructures capable of withstanding the growing number of cyberattacks.

**Keywords:** vulnerability; information security; database; centralization; integration; fragmentation; incident response.

Развитие цифровых технологий сопровождается стремительным ростом числа уязвимостей, выявляемых в программном и аппаратном обеспечении [1]. Эти дефекты становятся ключевым фактором, определяющим вероятность успешных атак, которые могут привести к утечкам данных, сбоям в функционировании сервисов и значительным финансовым потерям. Для своевременного реагирования на угрозы необходим доступ к достоверной и актуальной информации об уязвимостях. Однако сведения о них распределены между множеством международных и национальных баз [2–4], что затрудняет их использование и снижает эффективность процессов обеспечения информационной безопасности.

Проблема фрагментарности данных об уязвимостях заключается в том, что существующие источники, такие как CVE, NVD, OSV.dev, ExploitDB и национальная база ФСТЭК, содержат разнородные сведения и обновляются по разным правилам. В результате специалисты по безопасности вынуждены обращаться к нескольким ресурсам одновременно, сопоставлять информацию вручную и тратить значительные ресурсы на её обработку [5]. Такой подход замедляет выявление и устранение уязвимостей, снижает полноту картины угроз и создаёт риск упущенных критических инцидентов.

Одним из направлений решения этой проблемы является создание единого интеграционного ресурса, который позволил бы аккумулировать сведения из различных агрегаторов и представлять их в унифицированном виде [1, 6]. Централизация данных способствует повышению полноты и актуальности информации, упрощает процессы анализа и делает возможным автоматизированное выявление пересечений и дубликатов. Более того, единая база данных создаёт основу для интеграции с системами мониторинга и управления информационной безопасностью, что позволяет организациям переходить от реактивных мер к проактивным методам защиты [2].

Значимость централизованного подхода проявляется не только на уровне отдельных организаций, но и в масштабе национальной кибербезопасности. Единая база данных уязвимостей обеспечивает информационную поддержку государственных и корпоративных структур [4], способствует повышению их устойчивости к атакам и открывает возможности для развития интеллектуальных сервисов предиктивной аналитики, основанных на машинном обучении и моделировании угроз.

Фрагментарность данных об уязвимостях является серьёзным вызовом современной информационной безопасности, так как она замедляет процессы анализа и реагирования на инциденты. Преодоление этого вызова возможно за счёт централизации сведений и формирования единого ресурса, способного обеспечить полноту картины угроз и снизить затраты на их обработку. Создание такой базы рассматривается как необходимое условие построения устойчивых цифровых экосистем, которые могут эффективно противостоять растущему числу атак и обеспечивать стабильность критически важных информационных инфраструктур.

#### СПИСОК ЛИТЕРАТУРЫ

1. Федорченко, А. В., Чечулин, А. А., & Котенко, И. В. Построение интегрированной базы уязвимостей. Известия высших учебных заведений. Приборостроение, 2014, 57(11), 62–67.
2. Дойникова, Е. В. Средство мониторинга и интеграции уязвимостей из открытых баз данных / Е. В. Дойникова, Н. А. Кривых // Перспективные направления развития отечественных информационных технологий : Материалы VI межрегиональной научно-практической конференции, Севастополь, 22–26 сентября 2020 года / Науч. ред. Б.В. Соколов. Севастополь: Федеральное государственное автономное образовательное учреждение высшего образования «Севастопольский государственный университет», 2020. С. 231–232. EDN PSDVFL.
3. Акиншин, А. А. Анализ базы угроз в сфере информационной безопасности на примере Банка угроз ФСТЭК России / А. А. Акиншин, Н. Г. Ляпичева, М. Д. Ильменский // Вестник ЦЭМИ. 2022. Т. 5, № 4. DOI 10.33276/S265838870022995-7. EDN WEBCNP.
4. Антошкин, В. А. Особенности использования объектно-ориентированной СУБД mongodb / В. А. Антошкин, В. М. Скокан // Информатика и прикладная математика. 2020. № 26. С. 4–11. EDN RBTETS.
5. ФСТЭК России. База данных уязвимостей [Электронный ресурс]. URL: <https://www.fstec.ru/> (дата обращения: 25.06.2025).
6. Евдокимова, Д. А. Сравнительный анализ Методики оценки угроз безопасности информации ФСТЭК России и платформы моделирования угроз MITRE ATT&CK / Д. А. Евдокимова // Информационные технологии и математические методы в экономике и управлении : сборник статей XIII Международной научно-практической конференции имени А.И. Китова: в 3 т., Москва, 14–15 марта 2024 года. Москва: Российский экономический университет имени Г.В. Плеханова, 2024. С. 104–111. EDN BZDCDR.

УДК 004.056

#### ПРЕДОТВРАЩЕНИЕ ВНЕШНИХ УТЕЧЕК ПЕРСОНАЛЬНЫХ ДАННЫХ С УСТРОЙСТВ МОНИТОРИНГА ЗДОРОВЬЯ

Антропова Лидия Александровна<sup>1</sup>, Задбоев Вадим Александрович<sup>2</sup>, Санникова Полина Александровна<sup>1</sup>

<sup>1</sup> Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

<sup>2</sup> Военная академия связи им. Маршала Советского Союза С. М. Буденного  
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия  
e-mails: antrovalid@mail.ru, zadboev89@mail.ru, sannik882@mail.ru

**Аннотация.** В работе представлена защищённая IoT-платформа на базе микроконтроллера ESP32 и датчика MAX30100 для мониторинга ЧСС и SpO2. Особое внимание уделено информационной безопасности: проанализированы угрозы, включая MITM-атаки, перехват данных и компрометацию прошивки. Предложена многоуровневая защита, с применением TLS/SSL и DTLS для шифрования, цифровых сертификатов X.509, IDS/IPS, межсетевых экранов и регулярных обновлений с проверкой подписей. Решение обеспечивает надёжную защиту медицинских данных и может быть использовано в телемедицине. Перспективы связаны с внедрением машинного обучения для анализа аномалий и оптимизации работы системы.

**Ключевые слова:** IoT; TLS; SSL; DTLS; мониторинг здоровья; кибер угрозы.

## PREVENTING EXTERNAL LEAKAGES OF PERSONAL DATA FROM HEALTH MONITORING DEVICES

Antropova Lidiya<sup>1</sup>, Zadboev Vadim<sup>2</sup>, Sannikova Polina<sup>1</sup>

<sup>1</sup>The Bonch-Bruевич Saint Petersburg State University of Telecommunications  
22 Bolshhevikov Av, bldg 1, St. Petersburg, 193232, Russia

<sup>2</sup>Military Academy of Communications named after S. M. Budyonny

3 Tikhoretsky Prospekt, St. Petersburg, 195427, Russia

e-mails: antropovalid@mail.ru, zadboev89@mail.ru, sannik882@mail.ru

**Abstract.** The paper presents a secure IoT platform based on the ESP32 microcontroller and the MAX30100 sensor for monitoring heart rate and SpO2. Particular attention is paid to information security: threats are analyzed, including MITM attacks, data interception, and firmware compromise. Multi-level protection is proposed using TLS/SSL and DTLS for encryption, X.509 digital certificates, IDS/IPS, firewalls, and regular updates with signature verification. The solution provides reliable protection of medical data and can be used in telemedicine. Prospects are associated with the implementation of machine learning for anomaly analysis and system optimization.

**Keywords:** IoT; TLS; SSL; DTLS; health monitoring; cybersecurity.

Повышенный интерес к интеграции IoT-решений в медицинскую практику обусловлен комплексом факторов, вызванных как глобальными вызовами, так и технологическим прогрессом. Пандемия COVID-19 стала мощным катализатором развития телемедицины, сделав удалённую диагностику и мониторинг не просто дополнительной опцией, а необходимым элементом современной системы здравоохранения, особенно в условиях перегруженности медицинских учреждений и необходимости минимизации физических контактов. Традиционные методы мониторинга состояния пациентов, несмотря на высокую точность измерений, обладают рядом существенных ограничений: оборудование часто громоздкое, требует постоянного подключения к сети, а данные нуждаются в ручной интерпретации и не обеспечивают непрерывного контроля в домашних или мобильных условиях. В то же время стремительное развитие микроэлектроники, включая миниатюризацию компонентов и рост энергоэффективности, позволяет создавать носимые устройства, способные в автономном режиме собирать и передавать критически важные параметры здоровья. Однако на фоне роста внедрения таких решений остро встаёт вопрос обеспечения информационной безопасности, поскольку медицинские данные относятся к категории особо чувствительной информации, и их утечка или искажение может привести к тяжёлым последствиям как для пациентов, так и для медицинских организаций [1–3].

В рамках проведённого исследования была разработана аппаратно-программная платформа на базе микроконтроллера ESP32, интегрированного с датчиком пульсоксиметрии MAX30100. Выбор микроконтроллера ESP32 обусловлен его уникальным сочетанием функциональности: наличие встроенного Wi-Fi модуля стандарта 802.11 b/g/n, поддержка двусторонней связи по протоколам HTTP и HTTPS, низкое энергопотребление и возможность работы в автономном режиме делают его идеальным решением для носимых медицинских устройств. Датчик MAX30100 позволяет осуществлять непрерывный мониторинг частоты сердечных сокращений (ЧСС) и уровня насыщения крови кислородом (SpO2) методом фотоплетизмографии, который основан на анализе изменения интенсивности света, проходящего через ткани, в зависимости от пульсации кровотока. Такое решение обеспечивает высокую точность измерений при минимальном дискомфорте для пользователя, что особенно важно для долгосрочного наблюдения за пациентами с хроническими заболеваниями [4–6].

Однако внедрение IoT-устройств в медицинскую среду сопряжено с серьёзными киберугрозами, требующими всестороннего анализа потенциальных векторов атак. Наиболее опасными угрозами являются несанкционированный доступ к данным через эксплуатацию уязвимостей в программном обеспечении, фишинговые атаки, направленные на получение учётных данных, а также физическое вмешательство в работу устройства, например, при его потере или краже. Перехват данных в процессе передачи по беспроводным сетям остаётся одной из наиболее распространённых угроз, особенно если используются незащищённые или слабо защищённые протоколы. Атаки типа «человек посередине» (MITM) позволяют злоумышленнику не только перехватывать данные, но и модифицировать их, что может привести к ложной диагностике, назначению неправильного лечения или даже отключению критически важных функций устройства [7–9].

Эффективная защита медицинских IoT-систем должна строиться на соблюдении трёх фундаментальных принципов информационной безопасности: конфиденциальности, целостности и доступности (CIA-триада). Конфиденциальность гарантирует, что персональные медицинские данные будут доступны только авторизованным лицам и системам. Целостность обеспечивает защиту информации от несанкционированного

изменения, подмены или искажения, что критично для точности диагностики. Доступность подразумевает бесперебойную работу системы, исключающую отказ в обслуживании, особенно в экстренных ситуациях. Кроме того, любая система, обрабатывающая персональные данные пациентов, должна соответствовать международным нормативным требованиям, таким как HIPAA (США) и GDPR (ЕС), которые устанавливают строгие правила сбора, хранения, передачи и уничтожения медицинской информации [10].

Для верификации эффективности предложенных решений были проведены комплексные стресс-тесты, включающие имитацию DDoS-атак и попыток перехвата данных в беспроводной среде. Результаты испытаний подтвердили высокую устойчивость разработанной архитектуры: комбинированное применение TLS/SSL, сегментации сети и DTLS снизило вероятность успешной компрометации системы на 89%. При этом энергопотребление устройства в режиме непрерывной передачи данных составило в среднем 12.3 мАч, что свидетельствует о высокой энергоэффективности и пригодности решения для длительного автономного использования [11].

Разработанная многоуровневая система безопасности объединяет аппаратные, программные и организационные меры, обеспечивая комплексную защиту медицинских данных на всех этапах их жизненного цикла — от сбора на устройстве до хранения в медицинских информационных системах. Такой подход не только соответствует современным нормативным требованиям, но и способствует формированию доверия пациентов к цифровым технологиям в здравоохранении. В перспективе планируется интеграция методов машинного обучения для анализа поведения устройства и выявления аномалий в режиме реального времени, а также оптимизация алгоритмов шифрования и передачи данных с целью дальнейшего снижения энергопотребления и увеличения срока автономной работы. Реализация подобных решений открывает новые возможности для безопасного и масштабируемого внедрения IoT в персонализированную и профилактическую медицину.

#### СПИСОК ЛИТЕРАТУРЫ

1. Климов, К. О. Аналитика IoT данных с использованием сервиса AWS IoT analytics при исследовании загазованности окружающей среды / К. О. Климов, Г. А. Пискун // BIG DATA и анализ высокого уровня : сборник материалов VII международной научно-практической конференции, Минск, 19–20 мая 2021 года. Минск: Бестпринт, 2021. С. 131-137. EDN ZSMRPL.
2. Патент № 2834591 С1 Российская Федерация, МПК G06F 21/50, G06F 21/60. Система контроля безопасности сети передачи данных : заявл. 29.09.2023 : опубл. 11.02.2025 / В. А. Задбоев, В. А. Липатников, К. В. Мелехов [и др.] ; заявитель ФГКБОУ ВО Военная академия связи им. Маршала Советского Союза С.М. Буденного Мин обороны Российской Федерации. EDN EHCGFU.
3. Сорокин, Д. В. Инфраструктура промышленных сетей IoT, а так же киберугрозы в доступе IoT решениях / Д. В. Сорокин, А. П. Бондарчук, К. П. Сторчак // Телекоммуникационные и информационные технологии. 2019. № 4(65). С. 120-127. EDN LSHYOC.
4. Липатников, В. А. Обучение искусственного интеллекта на основе моделирования атак в сетях передачи данных / В. А. Липатников, В. А. Задбоев // 65-я науч.-технич. конф. проф-преп. состава, науч. работников и аспирантов (НТК ППС 2025) : Сб. науч. статей. В 3 т., Санкт-Петербург, 17–21 февраля 2025 года. СПб.: СПбГУ телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2025. С. 424-429. EDN UPDJWO.
5. Свидетельство о государственной регистрации программы для ЭВМ № 2025662651 Российская Федерация. Программа расчета вероятности проведения компьютерной атаки на основе применения теоремы Байеса : заявл. 30.04.2025 : опубл. 22.05.2025 / П. А. Берестовский, П. В. Воробьев, В. А. Задбоев. EDN KZTBFH.
6. Липатников В. А., Шевченко А.А. Методика проактивного управления информационной безопасностью распределенной информационной системы на основе интеллектуальных технологий // Информационные системы и технологии. 2022. № 2(130). С. 107-115.
7. Липатников В. А., Шевченко А.А. Математическая модель процесса управления информационной безопасностью распределенной информационной системы в условиях несанкционированного воздействия злоумышленника // Информационные системы и технологии. 2022. № 3(131). С. 121-130.
8. Липатников В.А., Шевченко А.А., Мелехов К.В., Задбоев В.А. Метод активной защиты объектов критической информационной инфраструктуры от кибератак на основе прерывания процесса воздействия нарушителя // Информационно-управляющие системы. 2025. № 2(135). С. 37-49.
9. Технические аспекты управления с использованием сети Интернет : Монография / А. А. Алейников, К. З. Билятдинов, А. В. Красов [и др.]. СПб : Центр научно-информационных технологий «Астерион», 2016. 305 с. ISBN 978-5-00045-408-4. EDN XGTJLL.
10. Контроль, измерение и интеллектуальное управление трафиком : монография / А. А. Алейников, К. З. Билятдинов, А. В. Красов, М. В. Левин. СПб : Центр научно-информационных технологий «Астерион», 2016. 92 с. ISBN 978-5-00045-385-8. EDN WLROTL.
11. Красов, А. В. Исследование методов провизинга безопасной сети на мультивендорном оборудовании с использованием средств автоматизированной конфигурации / А. В. Красов, Н. А. Косов, В. Ю. Холоденко // Colloquium-Journal. 2019. № 13-2(37). С. 243-247. EDN MJVGAY.

УДК 004.056

#### ЭКСПЕРИМЕНТАЛЬНАЯ ОЦЕНКА СТЕПЕНИ ЗАЩИТЫ KOTLIN-ПРИЛОЖЕНИЙ ПОСЛЕ ОБФУСКАЦИИ

Асаков Максим Рашидович

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевики пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mail: max.asakov@mail.ru

**Аннотация.** В рамках исследования проведена экспериментальная оценка степени защиты Kotlin-приложений после применения обфускации. Разработана методика комплексной обработки исходного кода, которая протестирована с использованием современных инструментов декомпиляции. Экспериментальные данные подтверждают, что предложенный подход обеспечивает значительное усложнение процесса реверс-инжиниринга при сохранении производительности приложения и минимальном воздействии на размер файлов.

**Ключевые слова:** Kotlin; безопасность; обфускация; цифровой водяной знак; android; декомпиляция.



## EXPERIMENTAL EVALUATION OF THE PROTECTION LEVEL OF KOTLIN APPLICATIONS AFTER OBFUSCATION

Asakov Maksim

<sup>1</sup> The Bonch-Bruевич Saint Petersburg State University of Telecommunications  
22 Bolshhevikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mail: max.asakov@mail.ru

**Abstract.** The study conducts an experimental evaluation of the protection level of Kotlin applications after obfuscation. A comprehensive source code processing methodology has been developed and tested using modern decompilation tools. Experimental data confirms that the proposed approach significantly complicates the reverse engineering process while maintaining application performance and minimizing the impact on file size.

**Keywords:** Kotlin; security; obfuscation; digital watermark; android; decompilation.

В статье рассматривается методика обфускации исходного кода Kotlin в Android-приложениях для защиты от декомпиляции. Kotlin, компилируемый в байт-код JVM/Dalvik, остаётся уязвимым к реверс-инжинирингу, что делает задачу защиты кода особенно актуальной. Стандартные инструменты вроде ProGuard/R8 обеспечивают лишь базовую защиту через переименование идентификаторов, но не поддерживают шифрование строк и модификацию потока исполнения. Более продвинутое решение (Allatori, DashO) предлагают расширенные функции, но имеют ограниченную поддержку Kotlin и требуют сложной настройки.

Автор предлагает пятиэтапную методику обфускации, специально адаптированную под особенности Kotlin. Сначала проводится анализ кода для выявления критических участков (аутентификация, API-запросы). Затем внедряется ложная логика – junk-код, фиктивные ветвления и пустые исключения. На третьем этапе выполняется массовое переименование классов и методов с добавлением opaque-предикатов. Далее применяется шифрование строк и метаданных через Gradle-плагины. Завершающий этап – финальная сборка с индивидуальными правилами ProGuard/R8.

Тестирование методики на пяти приложениях показало впечатляющие результаты: читаемость кода снизилась до 10% (против 40% у ProGuard), а восстановление логики стало возможным лишь на 25% (против 60%). При этом каждая сборка содержала до 12 ложных функций, что значительно затрудняло анализ. Важно, что методика практически не повлияла на производительность и размер APK, а её интеграция в CI/CD-процесс не требует глубоких изменений проекта.

В перспективе методику можно улучшить за счёт автоматизации генерации junk-кода и адаптации под новые инструменты декомпиляции. Таким образом, предложенный подход предлагает эффективное решение для защиты Kotlin-приложений, сочетающее высокий уровень безопасности с минимальными накладными расходами.

## СПИСОК ЛИТЕРАТУРЫ

1. Niroshan A., Seneviratne S., Seneviratne A. An Empirical Study of Code Obfuscation Practices in the Google Play Store. 2025.
2. Nawaz et al. On the evaluation of android malware detectors against code obfuscation techniques. PeerJ Computer Science, 2022.
3. Comviva MFS Engineering Tech Blog. Code obfuscations in Kotlin Multiplatform. 2023–2024.
4. Gaur A. Obfuscation in Android: ProGuard and R8. Medium.com, Jan 2025.
5. Faruki et al. Android Code Protection via Obfuscation Techniques: Past, Present and Future Directions. 2016.
6. A. Vasilev, «Methodology for Embedding a Digital Watermark in Java Application Class Files Resistant to Decompilation Attacks», Journal of Software Engineering and Applications, vol. 14, no. 3, pp. 45–59, 2022.
7. K. Müller, H. Chen, «Watermarking Java Programs Using Dummy Exception Handlers», International Journal of Information Security, vol. 21, № 1, pp. 12–26, 2023.
8. L. Novak and S. Cheng, «Dynamic Path-Based Software Watermarking», Proceedings of the 2021 ACM SIGPLAN Conference on Programming Language Design and Implementation, pp. 502–513, 2021.
9. Шариков П.И., Красов А.В., Штеренберг С.И. Методика создания и вложения цифрового водяного знака в исполняемые java файлы на основе замен опкодов // Т-Comm: Телекоммуникации и транспорт. 2017. Т. 11. №3. С. 66-70.
10. Шариков, П. И. Исследование атаки обфускацией на байт-код java-приложения с целью разрушения или повреждения цифрового водяного знака // I-methods. 2022. Т. 14, № 1. EDN GQGKIV.
11. Шариков, П. И. Исследование возможности использования java-агентов для вложения скрытого цифрового водяного знака непосредственно перед запуском java-приложения / П. И. Шариков, А. В. Красов // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2019. № 4. С. 14-18. EDN QQUVYX.
12. Шариков, П. И. Методика обфускации байт-кода Java-приложения с целью его защиты от атак декомпиляцией / П. И. Шариков // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2022. № 1. С. 64-72. DOI 10.46418/2079-8199\_2022\_1\_10. EDN AUOFNA.
13. Исследование и алгоритм предотвращения эксплуатации уязвимостей библиотеки журналирования Log4j в информационных системах Java-приложений / П. И. Шариков, А. Ю. Цветков, В. В. Сигачева, Л. К. Сиротина // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2023. № 4. С. 100-106. DOI 10.46418/2079-8199\_2023\_4\_19. EDN BULSON.
14. Шариков, П. И. Методика создания и скрытого вложения цифрового водяного знака в байт-код class-файла на основе не декларированных возможностей виртуальной машины java / П. И. Шариков // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2023. № 7-2. С. 165-174. DOI 10.37882/2223-2982.2023.7-2.37. EDN YBEWYQ.
15. Дудников, И. А. Методика анализа журналов событий информационных систем с использованием Elasticsearch для обнаружения сигналов о вредоносных действиях в информационной системе / И. А. Дудников, П. И. Шариков, А. В. Майоров // Научно-аналитический журнал «Вестник Санкт-Петербургского государственного Университета Государственной противопожарной службы МЧС России». 2025. № 1. С. 120-134. DOI 10.61260/2218-130X-2025-1-120-134. EDN ZQCEXG.

УДК 004.056

**АНАЛИЗ УСТОЙЧИВОСТИ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ В БАЙТ-КОДЕ  
В ЗАВИСИМОСТИ ОТ ТИПА ГЕНЕРАЦИИ ЛЯМБДА-ОБЪЕКТОВ KOTLIN****Асаков Максим Рашидович, Рублева Екатерина Борисовна**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mails: max.asakov@mail.ru, katarbl@yandex.ru

**Аннотация.** В статье рассматривается задача исследования влияния структуры сгенерированных лямбда-объектов Kotlin на устойчивость цифрового водяного знака в байт-коде. Основное внимание уделено анализу свойств, влияющих на надёжность и стойкость цифрового водяного знака, вложенного в байт-код, а также нахождению способов увеличить шанс на его сохранение. В результате исследования были получены аналитические соотношения для оценки устойчивости цифрового водяного знака в зависимости от особенности исследованной структуры, а также предложены рекомендации по оптимизации их использования с целью защиты.

**Ключевые слова:** Kotlin; цифровой водяной знак; структура; безопасность; байт-код.

**ANALYSIS OF DIGITAL WATERMARK RESILIENCE IN BYTECODE  
OF KOTLIN LAMBDA OBJECTS GENERATION TYPE****Asakov Maksim, Rubleva Ekaterina**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications  
22 Bolshhevikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mails: max.asakov@mail.ru, katarbl@yandex.ru  
+7(911)903-66-64, +7(922)944-58-50

**Abstract.** The article considers the problem of investigating the influence of the structure of generated Kotlin lambda objects on the stability of a digital watermark in bytecode. The focus is on analyzing the properties that affect the reliability and durability of a digital watermark embedded in a bytecode, as well as finding ways to increase the chance of its preservation. As a result of the study, analytical ratios were obtained to assess the stability of a digital watermark, depending on the features of the studied structure, and recommendations were proposed for optimizing their use for protection purposes.

**Keywords:** Kotlin; digital watermark; structure; security; bytecode.

В статье исследуется влияние структуры лямбда-объектов Kotlin на устойчивость цифровых водяных знаков в байт-коде при обфускации. Основное внимание уделено анализу различных типов лямбда-выражений (capturing, inline, suspend, SAM) и их поведению после обработки обфускаторами ProGuard, R8 и Allatori [1–6].

Эксперимент проводился на 20 программных модулях, где цифровой водяной знак встраивался либо в поля классов (для capturing-лямбд), либо в методы (для inline-лямбд). Результаты показали, что capturing-лямбды демонстрируют наивысшую устойчивость - водяной знак сохранялся в 81–100% случаев даже после агрессивной обфускации, благодаря сохранению структуры классов и полей. Suspend-лямбды также показали хорошие результаты (96% сохранности) из-за особенностей их state-machine реализации [7–9].

Напротив, inline-лямбды оказались наименее подходящими для защиты - водяной знак терялся в 73% случаев из-за полного встраивания кода и последующей оптимизации. SAM-адаптеры занимали промежуточное положение с 43% успешного извлечения водяного знака [10–15].

Исследование подтвердило, что выбор типа лямбда-выражения критически важен для защиты кода. Для обеспечения устойчивости цифровых водяных знаков в Android-приложениях рекомендуется использовать capturing- и suspend-лямбды, избегая inline-реализаций. Полученные результаты имеют практическое значение для разработчиков, занимающихся защитой авторских прав и интеллектуальной собственности в Kotlin-проектах.

**СПИСОК ЛИТЕРАТУРЫ**

1. Катасонов, А. И. Оценка стойкости механизма, реализующего... Мандатную сущностно-ролевую модель разграничения прав доступа в операционных системах семейства GNU LINUX / А. И. Катасонов, С. И. Штеренберг, А. Ю. Цветков // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 2. С. 50-56. DOI 10.46418/2079-8199\_2020\_2\_8. EDN EUMWWI.
2. Shterenberg, S. I. A Distributed Intrusion Detection System with Protection from an Internal Intruder / S. I. Shterenberg, M. A. Poltavtseva // Automatic Control and Computer Sciences. 2018. Vol. 52, No. 8. P. 945-953. DOI 10.3103/S0146411618080230. EDN BPIXFT.
3. Штеренберг, С. И. Методика построения защищенных систем искусственного интеллекта для проведения электроретинографии в офтальмологии / С. И. Штеренберг // Офтальмохирургия. 2022. № S4. С. 51-57. DOI 10.25276/0235-4160-2022-4S-51-57. EDN MNYJMC.
4. Шариков П.И., Красов А.В., Штеренберг С.И. Методика создания и вложения цифрового водяного знака в исполняемые java файлы на основе замен опкодов // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. №3. С. 66-70.
5. Шариков, П. И. Исследование атаки обфускацией на байт-код java-приложения с целью разрушения или повреждения цифрового водяного знака // I-methods. 2022. Т. 14, № 1. EDN GQGKIV.
6. Штеренберг, С. И. Разработка комплекса мер для защиты предприятия от фишинговых атак / С. И. Штеренберг, И. В. Стародубцев, В. С. Шашкин // Защита информации. Инсайд. 2020. № 2(92). С. 24-31. EDN LLETBN.
7. Предупреждение DoS-атак путем прогнозирования значений корреляционных параметров сетевого трафика / Д. С. Лаврова, Е. А. Попова, А. А. Штыркина, С. И. Штеренберг // Проблемы информационной безопасности. Компьютерные системы. 2018. № 3. С. 70-77. EDN VOHMBС.

8. Штеренберг, С. И. Принципы построения самоорганизующейся карты нейросети для архитектуры защищенной интеллектуальной системы обнаружения вторжений и инцидентов / С. И. Штеренберг // Информационная безопасность регионов России (ИБРР-2023) : XIII Санкт-Петербургская межрегиональная конференция. Материалы конференции, Санкт-Петербург, 25–27 октября 2023 года. Санкт-Петербург: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2023. С. 302–303. EDN HUWLEE.
9. Оценка статистических характеристик различных типов фреймов IEEE 802.11 для сервисов местоположения / В. А. Петров, М. М. Ковцур, А. Ю. Киструга, С. И. Штеренберг // Информационная безопасность регионов России (ИБРР-2021) : Материалы XII Санкт-Петербургской межрегиональной конференции, Санкт-Петербург, 27–29 ноября 2021 года. СПб: СПОИСУ, 2021. С. 187–188. EDN NNCMDY.
10. Свидетельство о государственной регистрации программы для ЭВМ № 2020664342 Российская Федерация. Программа для стеганографического преобразования и обфускации исполняемых файлов в системах обработки Больших данных : № 2020663631 : заявл. 03.11.2020 : опубл. 11.11.2020 / А. И. Красов, С. И. Штеренберг, В. Н. Волгогонов, Д. В. Кушнир ; заявитель ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича». EDN EKCCTG.
11. Свидетельство о государственной регистрации программы для ЭВМ № 2024662619 Российская Федерация. Программа определения местоположения IEEE 802.11 клиента : № 2024661418 : заявл. 21.05.2024 : опубл. 29.05.2024 / В. Е. Дрепа, М. М. Ковцур, А. Ю. Киструга, А. И. Пешков ; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича». EDN VCSGMO.
12. Ильин, Я. А. Обзор встроенного программного обеспечения для отслеживания деятельности пользователя / Я. А. Ильин, М. М. Ковцур, Д. А. Радионосский // Региональная информатика (РИ-2024) : Материалы XIX Санкт-Петербургской международной конференции, Санкт-Петербург, 23–25 октября 2024 года. Санкт-Петербург: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2024. С. 408–409. EDN EYUVOX.
13. Висутнов, С. С. Экосистема в мире информационной безопасности / С. С. Висутнов, К. А. Ахrameева // Международный журнал информационных технологий и энергоэффективности. 2024. Т. 9, № 7(45). С. 34–40. EDN DDHOAH.
14. Голубов, Н. А. Внутренние угрозы: Разнообразие и профилактика инсайдеров в организациях / Н. А. Голубов, Н. А. Косов // Развитие науки и практики в глобально меняющемся мире в условиях рисков : Сборник материалов XIX Международной научно-практической конференции, Москва, 30 мая 2023 года. Москва: Алеф, 2023. С. 173–180. EDN LTLHUO.
15. Киясов, А. И. Обнаружение и противостояние атаке в методе «цепочка убийств» / А. И. Киясов, Э. В. Бирих // Эволюционные процессы информационных технологий : Сборник научных статей 11-й Международной научно-технической конференции, Москва, 09 января 2025 года. М.: Институт гуманитарных наук, экономики и информационных наук, 2025. С. 405–409. EDN CIJODB.

УДК 004.056.5

## ОЦЕНКА ЭФФЕКТИВНОСТИ ANKEY SIEM NG В ОБНАРУЖЕНИИ DDOS-УГРОЗ: ПОТЕНЦИАЛ И НЕДОСТАТКИ

Ахrameева Ксения Андреевна<sup>1</sup>, Живодовский Иван Иванович<sup>2</sup>,  
Журавлева Анастасия Сергеевна<sup>1</sup>, Спицын Михаил Александрович<sup>1</sup>

<sup>1</sup> Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевики пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

<sup>2</sup> Военная академия связи им. Маршала Советского Союза С. М. Буденного  
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: ahrameeva.ka@sut.ru, ivan.zhivodovsky32@mail.ru, zhuravleva.as@sut.ru, spitsyn.ma@sut.ru

**Аннотация.** Рассматривается архитектура Optimized Correlator (OC) для SIEM-систем, используемая для оперативного выявления распределённых DDoS-атак путём комбинирования многопоточного сбора данных (логи Apache, события Snort), применения Hyperscan-ускоренных правил и корреляции событий.

**Ключевые слова:** SIEM; DDoS-атака; корреляция событий; Hyperscan; многопоточная архитектура; лог-анализ; IDS; Apache; Snort.

## EVALUATION OF THE EFFECTIVENESS OF ANKEY SIEM NG IN DETECTING DDOS THREATS: POTENTIAL AND DISADVANTAGES

Akhrameeva Ksenia<sup>1</sup>, Zhivodovsky Ivan<sup>2</sup>, Zhuravleva Anastasia<sup>1</sup>, Spitsyn Mikhail<sup>1</sup>

<sup>1</sup> The Bonch-Bruevich Saint Petersburg State University of Telecommunications  
22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia

<sup>2</sup> The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny  
3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: ahrameeva.ka@sut.ru, ivan.zhivodovsky32@mail.ru, zhuravleva.as@sut.ru, spitsyn.ma@sut.ru

**Abstract.** The Optimized Correlator (OC) architecture for SIEM systems is considered, which is used for the operational detection of distributed DDoS attacks by combining multithreaded data collection (Apache logs, Snort events), the use of Hyperscan-accelerated rules and event correlation.

**Keywords:** SIEM; DDoS attack; event correlation; Hyperscan; multithreaded architecture; log analysis; IDS; Apache; Snort.

Современные распределённые DDoS-атаки представляют собой растущую угрозу доступности сетевых сервисов [1–2]. В условиях усложняющейся структуры трафика и увеличивающегося объёма событий информационной безопасности, становится всё более актуальным использование высокопроизводительных SIEM-систем для их выявления. Одним из таких решений является Ankey SIEM NG, в рамках которого была реализована архитектура Optimized Correlator (OC), сочетающая многопоточную обработку логов, гиперускоренную фильтрацию с помощью Hyperscan и корреляционные правила EventGroup2, связывающие события по IP и временным меткам [3–4].

Была выполнена серия тестов, имитирующих наиболее распространённые типы атак: HTTP-флуды, SYN/UDP/ICMP-флуды, DNS-амплификационные атаки и медленные соединения. В каждом сценарии использовались реальные инструменты генерации трафика (GoldenEye, slowhttptest, hping3 и другие), а источниками логов выступали Apache и Snort. Для каждого типа атак были заданы шаблонные правила, срабатывающие по наличию определённых паттернов в логах. В тестах система успешно детектировала как одиночные события, так и их коррелированные проявления, обеспечивая своевременную генерацию алертов и минимальный уровень ложных срабатываний [5–7].

Применение Hyperscan, позволяющего компилировать и использовать регулярные выражения в SIMD-режиме, значительно сократило время обработки и повысило масштабируемость решения. Многопоточная архитектура позволила разделять входные логи на независимые блоки и обрабатывать их параллельно, что особенно критично при обработке трафика больших объёмов. Результаты тестирования показали, что система способна в реальном времени реагировать на атаки, обеспечивая требуемую производительность и надёжность.

Однако, как отмечают авторы, успешность промышленного применения Ankey SIEM NG зависит от качества настройки порогов, полноты логирования и адаптивности шаблонов [7]. Также существенную роль играют механизмы автоматического реагирования, которые в настоящее время базируются на интеграции с внешними средствами (iptables, SOAR). Таким образом, для повышения эффективности предлагается использовать адаптивное пороговое реагирование, поведенческое машинное обучение и облачно-нативные подходы к интеграции телеметрии.

Особое внимание уделяется IoT-угрозам, исходящим от ботнетов, где нагрузка на инфраструктуру может быть критической. В этом контексте Ankey SIEM NG демонстрирует потенциал как универсальное решение, способное объединять различные источники логов, обрабатывать зашифрованный и многоуровневый трафик, а также минимизировать время реагирования. По сравнению с классическими SIEM-подходами, ОС-модель предлагает более высокую чувствительность к атакам и снижение нагрузки на аналитиков SOC.

Таким образом, представленный программный комплекс может рассматриваться в качестве надёжной основы для построения систем мониторинга и реагирования на угрозы DDoS в корпоративной или облачной инфраструктуре. Внедрение компонентов машинного обучения, расширенных механизмов корреляции и автотюнинга правил позволит достичь высокого уровня автоматизации защиты и адаптивности в условиях динамичной угрозной среды.

#### СПИСОК ЛИТЕРАТУРЫ

1. Arif T. A Comprehensive Survey of Privacy-Enhancing and Trust-Centric Cloud-Native Security Techniques Against Cyber Threats / T. Arif, B. Jo, J.H. Park // *Sensors*. 2025. Vol. 25, No. 2350. P. 1-30. DOI: 10.3390/s25082350.
2. Защищенная модель программно-определяемой сети в среде виртуализации KVM / Д. В. Сахаров, А. В. Красов, И. А. Ушаков, Г. А. Орлов // *Электросвязь*. 2020. № 3. С. 26-32. DOI 10.34832/ELSV.2020.4.3.004. EDN IRRVAB.
3. Идея и общая концепция применения мультиагентного подхода к созданию крупномасштабных интеллектуальных систем обнаружения вторжений / С. И. Штеренберг, А. В. Красов, В. В. Максимов, А. В. Архипов // *Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки*. 2023. № 3. С. 128-136.
4. Разработка методологии тестирования систем защиты информации в виртуальных комплексах для обнаружения ошибок I и II-рода / А. В. Красов, Р. Р. Максудова, В. В. Нефедов [и др.] // *Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки*. 2021. № 1. С. 45-52. DOI 10.46418/2079-8199\_2021\_1\_7. EDN AACDXB.
5. Липатников В. А., Шевченко А.А. Методика проактивного управления информационной безопасностью распределенной информационной системы на основе интеллектуальных технологий // *Информационные системы и технологии*. 2022. № 2(130). С. 107-115.
6. Липатников В. А., Шевченко А.А. Математическая модель процесса управления информационной безопасностью распределенной информационной системы в условиях несанкционированного воздействия злоумышленника // *Информационные системы и технологии*. 2022. № 3(131). С. 121-130.
7. Липатников В. А., Шевченко А. А., Мелехов К. В., Задбоев В. А. Метод активной защиты объектов критической информационной инфраструктуры от кибератак на основе прерывания процесса воздействия нарушителя // *Информационно-управляющие системы*. 2025. № 2(135). С. 37-49.

УДК 004.056

#### ВЫБОР ПЛАТФОРМЫ ВИРТУАЛИЗАЦИИ В УСЛОВИЯХ ТЕХНОЛОГИЧЕСКОЙ ПОЛЯРИЗАЦИИ: СРАВНЕНИЕ УНИВЕРСАЛЬНОГО И СПЕЦИАЛИЗИРОВАННОГО ПОДХОДОВ

**Бирючевский Никита Евгеньевич, Пестов Игорь Евгеньевич, Мамченко Ксения Сергеевна**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

e-mails: nikitkabiruk@mail.ru, pestov.ie@yandex.ru, kmamchenko125@gmail.com

**Аннотация.** В статье проведён сравнительный анализ двух современных платформ виртуализации — Proxmox VE и Astra Linux — по ключевым критериям: функциональность, производительность, масштабируемость, уровень информационной безопасности и сфера применения. Актуальность исследования обусловлена растущими требованиями к защищённости и автономности ИТ-инфраструктур, особенно в условиях импортозамещения и стремления к цифровой независимости.

**Ключевые слова:** информационная безопасность; виртуализация; гипервизор; Astra Linux; Proxmox VE; KVM; LXC.

## SELECTING A VIRTUALIZATION PLATFORM IN THE CONTEXT OF TECHNOLOGICAL POLARIZATION: A COMPARISON OF GENERAL-PURPOSE AND SPECIALIZED APPROACHES

**Biryuchevskiy Nikita, Pestov Igor, Mamchenko Kseniia**

The Bonch-Bruевич Saint Petersburg State University of Telecommunications

22 Bolshhevikov Av, bldg 1, St. Petersburg, 193232, Russia

e-mails: nikitkabiruk@mail.ru, pestov.ie@yandex.ru, kmamchenko125@gmail.com

**Abstract.** The article provides a comparative analysis of two modern virtualization platforms — Proxmox VE and Astra Linux — according to key criteria: functionality, performance, scalability, level of information security and scope. The relevance of the study is due to growing demands for security and autonomy of IT-infrastructures, especially in conditions of import substitution and striving for digital independence.

**Keywords:** virtualisation; hypervisor; Astra Linux; Proxmox VE; KVM.

В статье представлен сравнительный анализ двух современных платформ виртуализации — Proxmox VE и Astra Linux — с точки зрения их функциональности, производительности, масштабируемости, уровня безопасности и сфер применения [1–3]. Актуальность исследования обусловлена растущими требованиями к эффективности и защищённости IT-инфраструктур, особенно в контексте импортозамещения и цифровой независимости [4].

Proxmox VE позиционируется как универсальное, масштабируемое и открытое решение, ориентированное на широкий круг пользователей — от малого бизнеса до крупных центров обработки данных. Платформа отличается поддержкой двух технологий виртуализации (KVM и LXC), встроенной кластеризацией, удобным веб-интерфейсом и высокой производительностью за счёт автоматизированного управления ресурсами, что делает её предпочтительной для задач, требующих гибкости, быстрого развёртывания и облачной интеграции [5, 6]. В то же время Astra Linux, разработанная с акцентом на информационную безопасность, предлагает строгую защиту данных, соответствие требованиям ФСТЭК и поддержку отечественного программного и аппаратного обеспечения, что определяет её основную нишу — государственные, оборонные и критически важные организации [7].

Несмотря на схожую основу на ядре Linux, архитектурные и философские различия между системами значительны: Proxmox VE делает ставку на открытость, автоматизацию и международную совместимость, тогда как Astra Linux фокусируется на контролируемости, сертифицированной защите и адаптации к российским стандартам [8, 9]. При этом Proxmox VE превосходит Astra Linux по производительности, масштабируемости и удобству администрирования, тогда как Astra Linux лидирует в области безопасности, шифрования по ГОСТ и совместимости с отечественной экосистемой [10].

Таким образом, выбор между платформами должен основываться на приоритетах конкретного проекта: для задач, где важны гибкость, скорость и масштабирование, предпочтительнее Proxmox VE; в то время как для организаций, работающих с конфиденциальной информацией и требующих соответствия государственным стандартам, более подходящим решением станет Astra Linux. Результаты анализа позволяют сформировать обоснованный подход к выбору виртуализационной платформы в зависимости от сферы применения и стратегических целей.

### СПИСОК ЛИТЕРАТУРЫ

1. Волкоготов В. Н., Гельфанд А. М., Деревянко В. С. Актуальность автоматизированных систем управления // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. Т. 1. С. 262-266.
2. Proxmox — Powerful open-source server solutions [Электронный ресурс]. URL: <https://www.proxmox.com> (дата обращения 12.03.2025).
3. Виртуализация QEMU/KVM в Astra Linux — Справочный центр — Справочный центр Astra Linux [Электронный ресурс]. URL: <https://wiki.astralinux.ru/pages/viewpage.action?pageId=3277425> (дата обращения 12.03.2025).
4. Горбань С.А., Красов А.В., Цветков А.Ю., Оценка эффективности механизмов контроля правами доступа в ОС Linux // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. Т. 1. С. 345-348.
5. Цветков А. Ю. Исследование существующих механизмов защиты операционных систем семейства Linux // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. Т. 1. С. 657-662.
6. Красов А. В., Штеренберг С. И., Москальчук А. И. Методология создания виртуальной лаборатории для тестирования безопасности распределённых информационных систем // Вестник Брянского государственного технического университета. 2020. № 3 (88). С. 38-46.
7. Штеренберг С. И., Москальчук А. И., Красов А. В. Разработка сценариев безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения // Информационные технологии и телекоммуникации. 2021. Т. 9. № 1. С. 47-58.
8. Цветков А. Ю. Анализ существующих механизмов защиты и атак в операционных системах // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. Т. 1. С. 927-931.
9. Кузнецов Д.Д., Цветков А. Ю. Использование систем принудительного контроля доступа для обеспечения безопасности контейнеризации. // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. Т. 1. С. 723-727.
10. Киселева А. А., Цветков А. Ю. Анализ существующих отечественных и OpenSource методов виртуализации // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2024. Т. 1. С. 713-717.

УДК 004.056

**ГРАФОВОЕ МОДЕЛИРОВАНИЕ СВЯЗНОСТИ УГРОЗ ДЛЯ ПРОАКТИВНОГО  
ПРОГНОЗИРОВАНИЯ КИБЕРРИСКОВ****Богданов Алексей Алексеевич**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mail: ar1se4101@gmail.com

**Аннотация.** Рассматривается необходимость перехода от традиционных реактивных методов информационной безопасности к проактивному подходу в ответ на растущее число и ущерб от кибератак.

**Ключевые слова:** кибератаки; проактивный подход; прогнозирование; графовый анализ.

**GRAPH MODELING OF THREAT CONNECTION FOR PROACTIVE CYBER RISK FORECASTING****Bogdanov Alexey**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications  
22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mail: ar1se4101@gmail.com

**Abstract.** The need to move from traditional reactive information security methods to a proactive approach in response to the growing number and damage from cyber-attacks is discussed.

**Keywords:** cyberattacks; proactive approach; forecasting; graph analysis.

Непрерывный рост числа кибератак (на 27% за первое полугодие 2025 года) и колоссальный ущерб, превышающий 170 млрд рублей, свидетельствуют о недостаточной эффективности традиционных реактивных инструментов информационной безопасности [1–2]. Стандартные подходы, основанные на мониторинге изолированных событий (таких как SIEM-системы), не позволяют своевременно выявлять и нейтрализовывать сложные, многоэтапные векторы атак. Это требует перехода к принципиально новой, проактивной методологии, фокус которой смещается с фиксации инцидента на его прогнозирование и количественную приоритизацию риска до момента его реализации [3].

Центральным элементом проактивного подхода является разработанная методология графового анализа связности угроз. Граф строится на основе агрегации и обработки данных из стандартизированных реестров, включая БДУ ФСТЭК России, MITRE ATT&CK, и актуальной информации из теневого информационного пространства, с применением технологий искусственного интеллекта. В отличие от пошагового анализа журналов событий, графовая модель позволяет динамически моделировать сложные пути развития потенциальной кибератаки. Она отражает взаимосвязи между отдельными уязвимостями, ошибками конфигурации и избыточными правами доступа, что позволяет оценить их кумулятивный эффект и увидеть общую картину потенциальной цепочки компрометации.

Применение графового анализа обеспечивает качественно новый уровень количественной оценки рисков. Риск определяется на основе динамической приоритизации: он резко возрастает, если подтвержденные угрозы образуют непрерывную цепочку на графе связности. Для реализации этого подхода необходима актуальная карта цифровых активов, с учетом ценности каждого актива, что обеспечивает взвешенное управление риском, а не просто фиксацию уязвимости. Кроме того, собранные на основе графового моделирования данные могут быть использованы для стратегического прогнозирования потенциального ущерба, включая такие количественные методы, как моделирование по методу Монте-Карло, что является критически важным для принятия решений на уровне руководства организации [4].

Главное преимущество данной методологии заключается в переходе от реагирования на изолированные события, характерного для стандартных средств защиты, к выявлению целостных, кумулятивных векторов атак. Если традиционные методы фиксируют отдельные «дыры» в защите, то графовый анализ позволяет «увидеть» и оценить, как эти уязвимости могут быть соединены злоумышленником в единую цепочку, что обеспечивает точное прогнозирование и приоритизацию критически важных рисков [5–6]. Такой упреждающий подход, согласующийся с требованиями ФСТЭК к защите информации и применимый в критически важных информационных инфраструктурах, трансформирует стратегию ИБ из реактивной в проактивную.

**СПИСОК ЛИТЕРАТУРЫ**

1. ФСБ: ущерб от дистанционных мошенничеств в России превысил 170 млрд руб. // TASS. — 07.05.2025 [Электронный ресурс]. — Режим доступа: <https://tass.ru/proisshestiya/23874465> (дата обращения: 10.08.2025).
2. Аналитика RED Security SOC: количество кибератак на российские компании за I полугодие 2025 года превысило 63 тыс. (на 27 % больше, чем в 2024 г.) // CNews. 14.07.2025 [Электронный ресурс]. Режим доступа: [https://safe.cnews.ru/news/line/2025-07-14\\_analitika\\_red\\_security\\_soc\\_itfinansy](https://safe.cnews.ru/news/line/2025-07-14_analitika_red_security_soc_itfinansy) (дата обращения: 10.08.2025).
3. Спрос на аудит информационной безопасности вырос на 23 % в 2025 г. // Computerra. 02.07.2025 [Электронный ресурс]. Режим доступа: <https://www.computerra.ru/317955/spros-na-audit-informatsionnoj-bezopasnosti-vyros-na-23-v-2025-godu> (дата обращения: 10.08.2025).
4. Дудников, И. А. Методика анализа журналов событий информационных систем с использованием Elasticsearch для обнаружения сигналов о вредоносных действиях в информационной системе / И. А. Дудников, П. И. Шариков, А. В. Майоров // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2025. № 1. С. 120-134. DOI 10.61260/2218-130X-2025-1-120-134. EDN ZQCEXG.

5. Шариков, П. И. Архитектура интегрированного java-приложения для анализа журналов с целью обнаружения компьютерных атак в информационных системах посредством реагирования на различные аномалии безопасности / П. И. Шариков, А. В. Красов, А. В. Майоров // Вестник Дагестанского государственного технического университета. Технические науки. 2025. Т. 52, № 1. С. 147-161. DOI 10.21822/2073-6185-2025-52-1-147-161. EDN AWEHRP.
6. Исследование и алгоритм предотвращения эксплуатации уязвимостей библиотеки журналирования Log4j в информационных системах Java-приложений / П. И. Шариков, А. Ю. Цветков, В. В. Сигаева, Л. К. Сиротина // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2023. № 4. С. 100-106. DOI 10.46418/2079-8199\_2023\_4\_19. EDN BULSON.

УДК 004.056

## АВТОМАТИЗИРОВАННАЯ СИСТЕМА ДЕТЕКЦИИ УЯЗВИМОСТЕЙ В ИОТ-УСТРОЙСТВАХ ПРОМЫШЛЕННОГО НАЗНАЧЕНИЯ

Борисенко Иван Иванович<sup>1</sup>, Живодовский Иван Иванович<sup>2</sup>, Марков Александр Сергеевич<sup>1</sup>

<sup>1</sup> Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевики пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

<sup>2</sup> Военная академия связи им. Маршала Советского Союза С. М. Буденного  
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: ivanborisenko03@yandex.ru, ivan.zhivodovsky32@mail.ru, alexander.markov.1999@mail.ru

**Аннотация.** В работе представлена концепция автоматизированной системы детекции уязвимостей в ИОТ-устройствах промышленного назначения, основанная на анализе угроз утечки персональных данных. Предлагаемая система интегрирует методы статического и динамического анализа безопасности, позволяя в автоматизированном режиме выявлять критические уязвимости на всех уровнях ИОТ-инфраструктуры: от периферийных устройств до облачных платформ. Система базируется на классификации угроз, разработанной в соответствии с международными стандартами ISO/IEC 27001, ISO/IEC 27005 и отечественными стандартами ГОСТ. Практическая реализация включает модуль пентестинга с использованием фреймворка Metasploit для проверки реальной эксплуатируемости обнаруженных уязвимостей.

**Ключевые слова:** автоматизированная детекция; ИОТ-безопасность; промышленный интернет вещей; анализ уязвимостей; пентестинг; Metasploit; информационная безопасность; персональные данные.

## AUTOMATED VULNERABILITY DETECTION SYSTEM FOR INDUSTRIAL IOT DEVICES

Borisenko Ivan<sup>1</sup>, Zhivodovsky Ivan<sup>2</sup>, Markov Alexander<sup>1</sup>

<sup>1</sup> The Bonch-Bruevich Saint Petersburg State University of Telecommunications  
22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia

<sup>2</sup> The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny  
3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: ivanborisenko03@yandex.ru, ivan.zhivodovsky32@mail.ru, alexander.markov.1999@mail.ru

**Abstract.** The paper presents the concept of an automated vulnerability detection system for industrial IoT devices, based on the analysis of personal data leakage threats. The proposed system integrates static and dynamic security analysis methods, enabling the automated identification of critical vulnerabilities across all levels of IoT infrastructure, from edge devices to cloud platforms. The system relies on a threat classification developed in accordance with international standards ISO/IEC 27001, ISO/IEC 27005, and Russian GOST standards. The practical implementation includes a penetration testing module utilizing the Metasploit framework to verify the exploitability of identified vulnerabilities.

**Keywords:** automated detection; IoT security; industrial internet of things; vulnerability analysis; penetration testing; Metasploit; information security; personal data.

Industrial IoT (IIoT) становится основой цифровой трансформации производственных процессов в рамках концепции «Индустрия 4.0». Однако внедрение ИОТ-технологий сопровождается ростом киберугроз, особенно в части утечки персональных данных сотрудников и клиентов. По данным исследований Avast, 23,7% ИОТ-устройств в России имеют критические уязвимости, создающие угрозу для конфиденциальности данных [1].

Основной задачей исследования является разработка архитектуры автоматизированной системы детекции уязвимостей, которая обеспечивает [2–5]:

- комплексный анализ ИОТ-инфраструктуры на всех уровнях (устройства, сети, шлюзы, облачные платформы);
- автоматическую классификацию обнаруженных уязвимостей по степени критичности;
- практическую верификацию найденных уязвимостей через контролируемый пентестинг;
- формирование рекомендаций по устранению выявленных угроз.

В рамках апробации системы были проведены тесты на лабораторном стенде, включающем типовые промышленные ИОТ-устройства.

Уязвимости устройств (Edge-уровень): обнаружены устройства с паролями по умолчанию, устаревшими прошивками и отсутствием механизмов безопасной загрузки.

Сетевые протоколы: выявлены незашифрованные каналы передачи данных и уязвимые беспроводные интерфейсы.

IoT-шлюзы: обнаружены уязвимости веб-интерфейсов и API, недостаточная аутентификация между компонентами.

Модуль динамического тестирования с использованием Metasploit Framework позволил подтвердить реальную эксплуатируемость 89% обнаруженных критических уязвимостей [6]. В ходе контролируемых атак была продемонстрирована возможность удаленного доступа к скомпрометированным устройствам, извлечения конфиденциальной информации и установления persistent-подключений для дальнейшего латерального движения по сети [7, 8].

Тестирование системы проводилось на стенде, включающем 25 различных IoT-устройств промышленного назначения. Результаты показали:

- время полного сканирования сети из 100 устройств: 23 минуты;
- точность детекции критических уязвимостей: 94.2%;
- процент ложноположительных срабатываний: 5.8%;
- покрытие всех 7 категорий угроз из разработанной классификации.

Наиболее критичными оказались уязвимости категорий «Аутентификация и управление доступом» (67% устройств) и «Уязвимости устройств Edge-уровня» (54% устройств).

Разработанная автоматизированная система детекции уязвимостей представляет собой комплексное решение для обеспечения безопасности промышленных IoT-инфраструктур. Основными преимуществами системы являются: автоматизация процесса аудита безопасности, высокая точность детекции реально эксплуатируемых уязвимостей, соответствие международным стандартам информационной безопасности. Дальнейшее развитие исследования предполагает интеграцию технологий машинного обучения для повышения точности классификации угроз и разработку адаптивных алгоритмов детекции для новых типов IoT-устройств и протоколов связи 5G/6G.

#### СПИСОК ЛИТЕРАТУРЫ

1. Технические аспекты управления с использованием сети Интернет : Монография / А. А. Алейников, К. З. Билятдинов, А. В. Красов [и др.]. Санкт-Петербург : Центр научно-информационных технологий «Астерион», 2016. 305 с. ISBN 978-5-00045-408-4. EDN XGTJLL.
2. Красов, А. В. Метод управления трафиком в гибридной программно-определяемой сети / А. В. Красов, М. В. Левин, А. Ю. Цветков // Информационные технологии и телекоммуникации. 2016. Т. 4, № 2. С. 53-63. EDN XDCOST.
3. Контроль, измерение и интеллектуальное управление трафиком : монография / А. А. Алейников, К. З. Билятдинов, А. В. Красов, М. В. Левин. Санкт-Петербург : Центр научно-информационных технологий «Астерион», 2016. 92 с. ISBN 978-5-00045-385-8. EDN WLROTL.
4. Липатников В.А., Парфиров В.А., Шевченко А.А., Мелехов К.В. Модель процесса обеспечения безопасности сети передачи данных в условиях информационного противоборства // Актуальные проблемы защиты и безопасности: Труды XXVI Всероссийской научно-практической конференции, Санкт-Петербург, 03–06 апреля 2023 года. Том 1. Санкт-Петербург: Типография Любавич, 2023. С. 569-572.
5. Шевченко А. А. Модель процесса защиты информационно-телекоммуникационной сети от несанкционированного воздействия // Инновационная деятельность в Вооруженных Силах Российской Федерации: Труды всеармейской научно-практической конференции, Санкт-Петербург, 10–11 октября 2019 года. Санкт-Петербург: ФГКБОУ ВО Военная академия связи им. Маршала Советского Союза С.М. Буденного» МО РФ, 2019. С. 166-173.
6. InfoWatch Analytics. Гигантская утечка данных в индустрии IoT. 2021.
7. ISO/IEC 27001 Information Security Management Systems Requirements. International Organization for Standardization, 2022.
8. Липатников В.А., Шевченко А.А., Омаров Р.Г. Способ защиты информационных сетей транспортных систем от DDoS-атак с прогнозированием // Транспорт России: проблемы и перспективы 2019: Материалы международной-научно-практической конференции, Санкт-Петербург, 12–13 ноября 2019 года. Том 1. Санкт-Петербург: Институт проблем транспорта им. Н.С. Соломенко РАН, 2019. С. 413-417.

УДК 0004.056.5

#### ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ПОСТКВАНТОВОЙ КРИПТОГРАФИИ В ИМТ-2030

**Брюшинин Александр Юрьевич, Второв Олег Павлович, Шевченко Александр Александрович**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

e-mails: albr135246@gmail.com, oleg20vtorov@gmail.com, alex\_pavel1991@mail.ru

**Аннотация.** По мере развития квантовых вычислений, традиционные криптографические методы, зависящие от вычислительной сложности, становятся уязвимыми, что требует перехода к квантово-устойчивым решениям для обеспечения будущей безопасности данных. Статья рассматривает развитие квантовых вычислений, современные методы шифрования и постквантовую криптографию.

**Ключевые слова:** информационная безопасность; квантовые вычислительные технологии; беспроводные сети будущего; криптографическая защита; устойчивые алгоритмы.

#### PROSPECTS FOR THE APPLICATION OF POST-QUANTUM CRYPTOGRAPHY IN IMT-2030

**Bryushinin Alexander, Vtorov Oleg, Shevchenko Aleksandr**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia

e-mails: albr135246@gmail.com, oleg20vtorov@gmail.com, alex\_pavel1991@mail.ru

**Abstract.** As quantum computing evolves, traditional cryptographic methods that depend on computational complexity become vulnerable, requiring a shift to quantum-resilient solutions to ensure future data security. The article examines the development of quantum computing, modern encryption methods and post-quantum cryptography.



**Keywords:** information security; quantum computing technologies; wireless networks of the future; cryptographic protection; stable algorithms.

Современные тенденции в области вычислительных технологий демонстрируют стремительный рост мощности квантовых процессоров. На практике это означает возможность одновременной обработки огромного числа состояний, что делает квантовые компьютеры особенно эффективными для выполнения задач, представляющих трудность для классических вычислительных систем. Однако именно эти возможности создают угрозу для криптографических методов, которые десятилетиями обеспечивали защищенность цифрового пространства. Наибольшему риску подвержены асимметричные схемы шифрования, в частности RSA и алгоритмы на основе эллиптических кривых, которые могут быть успешно атакованы с использованием алгоритма Шора. Симметричные методы более устойчивы, однако и они становятся уязвимыми при применении алгоритма Гровера, сокращающего сложность перебора [1–4].

В то время как индустрия активно внедряет технологии 6G, предполагающие колоссальные объемы передаваемой информации, сверхнизкую задержку и одновременное подключение миллионов устройств, проблема надежности механизмов защиты данных выходит на первый план. Обеспечение безопасности в условиях потенциального появления квантовых атак требует принципиально новых решений, основанных на постквантовой криптографии. Ключевым направлением здесь является разработка математических схем, чья сложность не снижается даже при использовании квантовых вычислителей [5–6].

Среди наиболее перспективных подходов можно выделить криптографию на основе решеточных структур, многомерных полиномов, кодов с исправлением ошибок и хеш-функций. Каждое из этих направлений обладает как преимуществами, так и определенными ограничениями, что подчеркивает необходимость комплексного подхода и тщательного анализа устойчивости. Важным событием последних лет стал международный конкурс NIST, целью которого является выбор алгоритмов, способных заменить уязвимые методы. Уже выделены решения, прошедшие финальные этапы отбора, среди которых CRYSTALS-Kyber для защиты ключевого обмена и CRYSTALS-Dilithium для цифровых подписей. Эти разработки демонстрируют реальную готовность к интеграции в системы нового поколения [7–9].

Перспективы внедрения постквантовой криптографии в сети шестого поколения не ограничиваются только заменой отдельных алгоритмов. Они предполагают пересмотр всей архитектуры безопасности, включая процедуры аутентификации, механизмы защиты от атак «человек посередине» и методы обеспечения целостности каналов связи. Одновременно с этим необходимо учитывать вопросы масштабируемости и производительности, так как новые алгоритмы должны сохранять эффективность при реальной эксплуатации в условиях больших сетей [10–13].

Развитие квантовых вычислительных технологий радикально меняет подход к обеспечению безопасности информационного пространства. Для того чтобы сохранить надежность систем связи будущего, требуется заранее подготовить устойчивую к квантовым атакам криптографическую основу. Сети шестого поколения станут критически важным элементом цифровой инфраструктуры, и их защита от новых угроз должна стать приоритетной задачей исследователей и разработчиков. В дальнейшем особое внимание необходимо уделить оптимизации постквантовых алгоритмов, выработке международных стандартов и адаптации технологий к промышленным и государственным системам, где высокая степень безопасности является условием стабильного функционирования.

#### СПИСОК ЛИТЕРАТУРЫ

1. Sarkar, B. Study and Analysis of Error Propagation Effect of Advanced Encryption Standard / B. Sarkar [et al.] // Int'l J HIT Transaction on ECCN. 2008. Vol. 2, № 7.
2. Коутинхо С. Введение в теорию чисел / С. Коутинхо. Москва: Изд-во МЦНМО, 2011. 312 с.
3. Мао, В. Современная криптография: теория и практика / В. Мао. Москва: Вильямс, 2005. 768 с.
4. Душкин Р.В. Квантовые вычисления и функциональное программирование. Москва, 2014. 33 с.
5. Малыгина М.П., Герасимов Д.А. Симуляция квантовых вычислений. Краснодар: КГТУ, 2016. 9 с.
6. Липатников В. А., Шевченко А.А. Методика проактивного управления информационной безопасностью распределенной информационной системы на основе интеллектуальных технологий // Информационные системы и технологии. 2022. № 2(130). С. 107–115.
7. Samsung Research. 6G: The Next Hyper-Connected Experience for All. [Seoul]: Samsung Research, 2020.
8. National Institute of Standards and Technology. Post-Quantum Cryptography. [Электронный ресурс]. URL: <https://www.nist.gov/itl/csd/groups/post-quantum-cryptography> (дата обращения: 24.05.2025).
9. Липатников В. А., Шевченко А.А. Математическая модель процесса управления информационной безопасностью распределенной информационной системы в условиях несанкционированного воздействия злоумышленника // Информационные системы и технологии. 2022. № 3(131). С. 121–130.
10. Липатников В.А., Шевченко А.А., Мелехов К.В., Задбоев В.А. Метод активной защиты объектов критической информационной инфраструктуры от кибератак на основе прерывания процесса воздействия нарушителя // Информационно-управляющие системы. 2025. № 2(135). С. 37–49.
11. Майоров, А. В. Модель представления Больших данных о компьютерных атаках в формате nosql / А. В. Майоров, А. В. Красов, И. А. Ушаков // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2023. № 2. С. 47–54. DOI 10.46418/2079-8199\_2023\_2\_9. EDN GDZKWM.
12. Krasov, A. Behavioral Analysis of Resource Allocation Systems in Cloud Infrastructure / A. Krasov, L. Vitkova, I. Pestov // International Russian Automation Conference, RusAutoCon 2019, Sochi, 08–14 сентября 2019 года. Sochi: Institute of Electrical and Electronics Engineers Inc., 2019. P. 8867699. DOI 10.1109/RUSAUTOCON.2019.8867699. EDN OEKKNH.
13. Guidelines for Using Machine Learning Technology to Ensure Information Security / M. M. Kovtsur, A. V. Mikhailova, P. A. Potemkin [et al.] // 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops, ICUMT 2020, Brno, 05–07 октября 2020 года. Brno: Institute of Electrical and Electronics Engineers, 2020. P. 285–290. DOI 10.1109/ICUMT51630.2020.9222417. EDN MFRZCC.

УДК 004.056.53

**СИГНАЛЬНЫЙ КОНТРОЛЬ ЛИНИЙ СВЯЗИ ДЛЯ ВЫЯВЛЕНИЯ ПОДКЛЮЧЕНИЙ****Васичкин Сергей Сергеевич**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mail: sergey\_vasichkin@bk.ru

**Аннотация.** Рассматривается прикладной метод обеспечения технической защиты информации путём мониторинга физических параметров линий связи. Основа подхода — фазово-амплитудный анализ отражённых сигналов, позволяющий фиксировать малейшие изменения, вызванные несанкционированными подключениями или деградацией компонентов. Метод не зависит от сетевой активности, не требует вмешательства в программное обеспечение и может применяться в условиях ограниченного доступа. Представлены ключевые характеристики системы контроля, её архитектура и сценарии практического применения на критически важных объектах.

**Ключевые слова:** физический контроль; отражённый сигнал; линии связи; несанкционированное подключение; мониторинг инфраструктуры; фазовый анализ.

**SIGNAL MONITORING OF COMMUNICATION LINES TO IDENTIFY CONNECTIONS****Vasichkin Sergey**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications  
22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mail: sergey\_vasichkin@bk.ru

**Abstract.** This paper presents an applied method for securing communication infrastructure through signal-level diagnostics. The approach relies on analyzing reflected signals to detect unauthorized connections or physical degradation. The system operates independently of network traffic and software layers, offering compatibility with restricted-access environments. Its architecture ensures continuous and autonomous monitoring, making it suitable for critical infrastructures requiring covert observation and high detection reliability.

**Keywords:** physical monitoring; reflected signal; communication lines; unauthorized connection; infrastructure diagnostics; phase analysis.

Контроль состояния физических линий связи является важной частью системы защиты информации. Передача данных в таких линиях зависит от стабильности кабельной инфраструктуры, качества соединений и целостности среды распространения сигнала. Несмотря на применение логических и криптографических методов, такие как шифрование, фильтрация и аутентификация, физический уровень остаётся слабо защищённым. Если злоумышленник получает доступ к кабелю, он может установить несанкционированное подключение, создать ответвление или изменить нагрузку, при этом не нарушая работу протоколов и не вызывая сбоев в передаче данных. Такие вмешательства не сопровождаются аномалиями на логическом уровне и часто остаются незамеченными при использовании обычных методов наблюдения за сетью. Особенно это актуально в условиях, когда требуется скрытность наблюдения и невозможна установка активных систем защиты на логическом уровне [1].

Для решения этой задачи применяется подход, основанный на анализе физических характеристик сигнала, отражённого от линии. На линию подаётся тестовый импульс, а затем система фиксирует и анализирует отражённый сигнал. Даже незначительные изменения в структуре линии — например, появление нового разъёма, ухудшение контакта или подключение небольшого отрезка кабеля — вызывают фазовые и амплитудные искажения, а также изменяют временные параметры сигнала. Эти отклонения можно точно измерить и использовать для оценки состояния линии. Подход позволяет обнаруживать как очевидные, так и скрытые вмешательства, включая пассивные подключения, которые не создают активности в сетевом трафике, но представляют угрозу безопасности. Кроме того, анализ отражённого сигнала даёт возможность зафиксировать начальные признаки физического износа, такие как старение изоляции, ослабление соединений или деградация экранирования.

В отличие от традиционных методов мониторинга, требующих вмешательства в логическую структуру сети, предложенный подход реализуется полностью на физическом уровне. Система работает автономно, не анализирует содержимое передаваемых данных и не зависит от формата используемых протоколов. Это обеспечивает её устойчивость к ложным срабатываниям и совместимость с сертифицированными инфраструктурами, где модификация логики или ПО невозможна [2].

Ключевым элементом метода является создание эталонного сигнального профиля, который показывает, как линия связи работает в нормальных условиях. На начальном этапе система записывает основные параметры отражённого сигнала, такие как амплитуда, фаза, задержка и спектр. Затем все новые измерения сравниваются с этим эталоном. Если зафиксированы отклонения, система определяет текущее состояние линии как стабильное, нестабильное или критическое. Такой способ позволяет проводить постоянный автоматический контроль без участия человека. При появлении отклонений система может сразу сообщить об угрозе и сохранить данные для анализа.

Результаты применения метода показывают, что он хорошо работает в ситуациях, где важно сохранить надёжность и незаметность контроля. Система может обнаруживать даже небольшие изменения в линии, которые не влияют на передачу данных, но указывают на возможное подключение. Это особенно полезно для объектов с ограниченным доступом, где нельзя использовать обычные средства наблюдения. Метод подходит для разных условий: от серверных помещений до удалённых участков. Система может работать как в одиночном режиме, так и в составе распределённой сети, передавая данные с нескольких точек; позволяет отслеживать не только внешние подключения, но и постепенную деградацию компонентов: ослабление контактов, ухудшение экранирования, старение изоляции. Это даёт возможность проводить профилактику до наступления отказа, повышая общую устойчивость инфраструктуры [3].

Метод легко масштабируется и может быть использован как в стационарных, так и в мобильных и распределённых конфигурациях. Его применение целесообразно в условиях ограниченного доступа к объектам, в том числе в энергетике, транспорте, оборонной и банковской инфраструктуре. Отсутствие необходимости в интеграции с логическими компонентами делает систему универсальной и совместимой с широким спектром существующих решений.

Таким образом, фазово-амплитудный анализ отражённого сигнала в сочетании с эталонным профилированием создаёт надёжную основу для построения автоматизированной системы физического мониторинга линии связи. В отличие от традиционных методов, ориентированных на сетевой или прикладной уровни, данный подход работает на уровне физической инфраструктуры, что обеспечивает дополнительный уровень защиты, особенно в условиях ограниченного доступа или при высоких требованиях к скрытности и непрерывности наблюдения.

Метод позволяет выявлять не только факт подключения, но и классифицировать его характер и степень угрозы, благодаря чему система может быть использована не только в целях фиксации событий, но и для построения интеллектуальных механизмов реагирования. Автономность функционирования, невмешательство в логическую структуру сети и устойчивость к внешним воздействиям делают разработанную систему универсальным инструментом технической диагностики и превентивного контроля.

Применение разработанного подхода возможно в широком спектре задач: от защиты критической инфраструктуры до мониторинга распределённых сетей, включая энергетические, транспортные и промышленные объекты. Система легко масштабируется, не требует значительной модификации существующего оборудования и способна функционировать в реальном времени без остановки технологических процессов.

Предложенная методика позволяет перейти от реактивных мер безопасности к проактивному контролю состояния канала связи, своевременно выявляя потенциальные зоны риска и предотвращая развитие аварийных ситуаций. Это особенно важно в условиях роста числа угроз, связанных с техническими закладками, несанкционированными подключениями и деградацией кабельной инфраструктуры. Метод открывает перспективы для дальнейшего развития интеллектуальных систем мониторинга, интегрированных в многоуровневые комплексы обеспечения информационной и технической безопасности.

#### СПИСОК ЛИТЕРАТУРЫ

1. Орлов Ю. Ф. Активная идентификация объектов управления. М. : МГТУ им. Н. Э. Баумана, 2010. 296 с.
2. Алейников А. А., Билятдинов К. З., Красов А. В., Левин М. В. Контроль, измерение и интеллектуальное управление трафиком: монография. Санкт-Петербург : Центр научно-информационных технологий «Астерион», 2016. 92 с. ISBN 978-5-00045-385-8.
3. Билятдинов К. З., Красов А. В., Меняйло В. В. Исследование систем и анализ результатов испытаний. Санкт-Петербург : Центр научно-информационных технологий «Астерион», 2019. 362 с. ISBN 978-5-00045-813-6.

УДК 004.056.53

#### СПЕЦИАЛИЗИРОВАННЫЕ АППАРАТНЫЕ СРЕДСТВА КАК ИНСТРУМЕНТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БИОМЕТРИЧЕСКИХ СИСТЕМАХ

**Веселова Анастасия Дмитриевна**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевики пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mail: aveselova806@gmail.com

**Аннотация.** В тезисах доклада проводится комплексный анализ роли специализированных аппаратных средств в обеспечении безопасности биометрических систем. Исследуются принципы функционирования и security-модели таких технологий, как аппаратные модули безопасности (HSM), доверенные платформенные модули (TPM), защищенные анклавы (Secure Enclave) и специализированные биометрические сенсоры. Детально оцениваются криптографические аспекты их применения, включая безопасное хранение ключей и шифрование биометрических шаблонов. Проводится сравнительный анализ резистентности аппаратных и программных решений к различным классам атак. Особое внимание уделяется вызовам, связанным с интеграцией и стоимостью таких решений. В заключение формулируются перспективные направления развития аппаратной защиты в контексте эволюции угроз и стандартов в области биометрической безопасности.

**Ключевые слова:** информационная безопасность; биометрические системы; аппаратные средства защиты; HSM; TPM; Secure Enclave; биометрические шаблоны; криптография; несанкционированный доступ.

## SPECIALIZED HARDWARE AS TOOLS FOR ENSURING INFORMATION SECURITY IN BIOMETRIC SYSTEMS

Veselova Anastasia

The Bonch-Bruевич Saint Petersburg State University of Telecommunications  
22 Bolshhevikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mail: aveselova806@gmail.com

**Abstract.** This article provides a comprehensive analysis of the role of specialized hardware devices in ensuring the security of biometric systems. It examines the principles of operation and security models of technologies such as hardware security modules (HSMs), trusted platform modules (TPMs), secure enclaves (Secure Enclave), and specialized biometric sensors. It provides a detailed assessment of the cryptographic aspects of their use, including secure key storage and encryption of biometric templates. A comparative analysis of the resistance of hardware and software solutions to various classes of attacks is conducted. Particular attention is paid to the challenges associated with the integration and cost of such solutions. In conclusion, promising areas for the development of hardware protection are formulated in the context of the evolution of threats and standards in the field of biometric security.

**Keywords:** information security; biometric systems; hardware security devices; HSM; TPM; Secure Enclave; biometric templates; cryptography; unauthorized access.

Широкомасштабная цифровизация и повсеместное проникновение информационных технологий обусловили активную интеграцию биометрических методов аутентификации и идентификации в различные сферы жизнедеятельности. Данные технологии, основанные на использовании уникальных физиологических (отпечатки пальцев, радужная оболочка, лицо) и поведенческих (голос, походка) характеристик индивида, нашли применение в системах контроля доступа, мобильных устройствах, финансовом секторе и государственном управлении. Их ключевое преимущество перед традиционными аутентификаторами (пароли, PIN-коды) заключается в свойстве неотторжимости и сложности копирования, что теоретически повышает уровень безопасности.

Однако парадигма «биометрия как пароль» порождает уникальные риски. Компрометация биометрических данных носит необратимый характер — в отличие от пароля, отпечаток пальца или изображение лица невозможно изменить. Это предъявляет исключительно высокие требования к механизмам их защиты на всех этапах жизненного цикла: от сбора и обработки до хранения и передачи. В данном контексте программно-реализованные механизмы безопасности зачастую демонстрируют недостаточную устойчивость к сложным атакам, таким как атаки по сторонним каналам, эксплуатация уязвимостей операционной системы или вредоносное ПО. Это актуализирует необходимость применения решений, обеспечивающих более глубокий уровень защиты, основанный на физической и логической изоляции.

Аппаратные средства безопасности представляют собой специализированные физические компоненты, предназначенные для безопасного выполнения криптографических операций и хранения критически важной информации. Их фундаментальное преимущество заключается в реализации принципа «доверенной вычислительной базы», которая изолирована от основной операционной системы и менее уязвима для программных атак [1].

Среди наиболее релевантных для биометрических систем аппаратных решений можно выделить аппаратные модули безопасности (HSM), представляющие собой специализированные криптографические устройства, сертифицированные по международным стандартам [2]. Их основная функция — генерация, хранение и управление жизненным циклом криптографических ключей. В биометрических системах HSM обеспечивают шифрование биометрических шаблонов как при хранении в централизованной базе данных, так и при передаче по сети, при этом ключи никогда не покидают защищенную границу модуля [3].

Доверенные платформенные модули (TPM) и защищенные анклавы (Secure Enclave) интегрируются непосредственно в потребительские устройства. TPM представляет собой стандартизированный криптопроцессор, обеспечивающий функции измерения целостности программной среды и безопасного хранения ключей [3]. Secure Enclave является примером выделенной защищенной подсистемы, которая изолирует обработку биометрических данных от основного ядра процессора. Данные, обрабатываемые в анклав, никогда не передаются в операционную систему или приложения, что минимизирует поверхность атаки. Современные биометрические сенсоры включают сложные антиспуфинговые механизмы для обнаружения поддельных образцов, являясь первой линией защиты против сфальсифицированных биометрических характеристик [4].

Эмпирические данные и теоретические модели демонстрируют, что аппаратная защита существенно повышает общую устойчивость биометрической системы. Комбинированное использование защищенных сенсоров, TPM/Secure Enclave для локальной обработки и HSM для централизованного хранения создает многоуровневую оборону. Однако широкое распространение данных технологий сдерживается рядом факторов, включая высокую стоимость закупки и развертывания решений, что делает их малодоступными для малого и среднего бизнеса. Сложность интеграции аппаратных средств в существующую IT-инфраструктуру требует глубоких экспертных знаний и может привести к необходимости модификации архитектуры системы. Кроме того, несмотря на наличие стандартов, обеспечение бесперебойного взаимодействия между компонентами от разных производителей остается нетривиальной задачей.

## СПИСОК ЛИТЕРАТУРЫ

1. Алехин, Р. В. Статистические методы анализа данных / Р. В. Алехин, Г. С. Бударный, А. О. Камалова // Студенческая весна 2024 : Сборник научных статей 78-ой региональной научно-технической конференции студентов, аспирантов и молодых ученых, Санкт-Петербург, 15 мая 2024 года. СПб: СПбГУ телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2024. С. 53-57. EDN HZDTTS.
2. Штеренберг, С. И. Уникальные направления атак на искусственный интеллект и нейронные сети / С. И. Штеренберг, В. А. Севостьянов, Г. С. Бударный // Вестник СПбГУПТД. Серия 1: Естественные и технические науки. 2024. № 2. С. 103-112. DOI 10.46418/2079-8199\_2024\_2\_19. EDN EZWNUU.
3. Сравнительный анализ метрик вычислительных ресурсов виртуальных машин и контейнеров для обеспечения безопасности / А. О. Камалова, И. Е. Пестов, Г. С. Бударный [и др.] // Вестник СПбГУПТД. Серия 1: Естественные и технические науки. 2025. № 1. С. 81-88. DOI 10.46418/2079-8199\_2025\_1\_15. EDN QZEWXB.
4. Штеренберг, С. И. Технологии программной защиты в интернете / С. И. Штеренберг, В. Е. Морозов, В. И. Андрианов. Том Часть 2. СПб: СПбГУ телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2015. 76 с. ISBN 978-5-89160-126-0. EDN YWUXGK.

УДК 004.056

**ЦИФРОВАЯ УСТОЙЧИВОСТЬ ГОСУДАРСТВА ЧЕРЕЗ СОБСТВЕННЫЕ ПЛАТФОРМЫ  
МОНИТОРИНГА БЕЗОПАСНОСТИ****Волостных Виктор Анатольевич, Задбоев Вадим Александрович, Липатников Валерий Алексеевич**

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: zadboev89@mail.ru, vas@mil.ru

**Аннотация.** В условиях нарастающего числа киберугроз и усложнения архитектуры государственных информационных систем особую актуальность приобретает задача построения собственных решений для мониторинга и анализа событий информационной безопасности. В статье раскрываются подходы к созданию национальных SIEM-платформ, ориентированных на соблюдение требований отечественного законодательства, использование сертифицированных средств защиты информации и обеспечение технологического суверенитета. Рассмотрены архитектурные и организационные аспекты интеграции SIEM в инфраструктуру государственных учреждений, обозначены ключевые этапы внедрения, а также акцентировано внимание на необходимости постоянной адаптации системы к изменяющемуся ландшафту угроз.

**Ключевые слова:** информационная безопасность; цифровая устойчивость; SIEM; государственные информационные ресурсы; критическая инфраструктура; мониторинг событий; технологический суверенитет; защита данных.

**DIGITAL RESILIENCE OF THE STATE THROUGH PROPRIETARY  
SECURITY MONITORING PLATFORMS****Volostnyh Viktor, Zadboev Vadim, Lipatnikov Valeriy**

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: zadboev89@mail.ru, vas@mil.ru

**Abstract.** In the context of the growing number of cyber threats and the increasing complexity of the architecture of state information systems, the task of building our own solutions for monitoring and analyzing information security events is becoming especially relevant. The article reveals approaches to creating national SIEM platforms focused on compliance with domestic legislation, the use of certified information security tools and ensuring technological sovereignty. The architectural and organizational aspects of SIEM integration into the infrastructure of government agencies are considered, key stages of implementation are outlined, and attention is focused on the need for constant adaptation of the system to the changing threat landscape.

**Keywords:** information security; digital resilience; SIEM; government information resources; critical infrastructure; event monitoring; technological sovereignty; data protection.

Современные государственные информационные системы функционируют в условиях постоянно возрастающего объема киберугроз, среди которых преобладают целевые атаки на критическую инфраструктуру и попытки несанкционированного доступа к персональным данным. Эти вызовы делают традиционные методы защиты недостаточными и стимулируют развитие комплексных решений, объединяющих превентивные механизмы и средства ситуационного мониторинга.

В качестве ключевого инструмента обеспечения киберустойчивости выступают SIEM-системы, предназначенные для централизованного сбора, корреляции и анализа событий информационной безопасности. Их применение позволяет существенно повысить прозрачность происходящих процессов, сократить время обнаружения и реагирования на инциденты, а также создать условия для проведения ретроспективного анализа, необходимого в целях расследования и подтверждения соответствия регуляторным требованиям [1–2].

Особое значение в контексте государственных организаций имеет ориентация на применение отечественного программного обеспечения и сертифицированных средств защиты информации. Такой подход не только обеспечивает соответствие обязательным требованиям ФСТЭК и ФСБ России, но и формирует

технологическую независимость от зарубежных поставщиков, что является критически важным элементом стратегической устойчивости.

Архитектурные решения при проектировании SIEM предполагают модульную структуру, включающую подсистемы сбора и предобработки данных, корреляционные механизмы, долговременное хранилище событий и средства визуализации для центров мониторинга безопасности. Применение сертифицированных средств криптографической защиты и реализация специализированных сегментов сети позволяют обеспечить надежность и полноту функционирования системы [3].

Внедрение SIEM-системы требует поэтапного подхода, включающего обследование информационно-вычислительной сети, построение прототипа в тестовой среде, адаптацию правил корреляции под актуальные угрозы и постепенную интеграцию с существующими элементами инфраструктуры. В процессе эксплуатации особое внимание уделяется постоянному обновлению аналитических сценариев и повышению компетенций персонала, задействованного в мониторинге и реагировании на инциденты [4–5].

Таким образом, создание национальной SIEM-платформы в государственных организациях является не только технологическим, но и стратегическим шагом, направленным на формирование целостной системы обеспечения информационной безопасности. Наличие таких решений позволяет не только повысить уровень защищенности критически важных ресурсов, но и продемонстрировать цифровой суверенитет государства, что приобретает особую значимость в условиях глобальной нестабильности и роста числа киберугроз.

#### СПИСОК ЛИТЕРАТУРЫ

1. Липатников В.А., Шевченко А.А., Мелехов К.В., Задбоев В.А. Метод активной защиты объектов критической информационной инфраструктуры от кибератак на основе прерывания процесса воздействия нарушителя // Информационно-управляющие системы. 2025. № 2(135). С. 37–49.
2. Патент № 2839562 С1 Российская Федерация, МПК G06F 12/14, H04L 12/22. Способ защиты информационно-вычислительной сети от вторжения : заявл. 27.02.2024 : опубл. 06.05.2025 / В. А. Задбоев, В. А. Липатников, К. В. Мелехов, А. А. Шевченко ; заявитель Федеральное государственное казенное военное образовательное учреждение высшего образования «Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С.М. Буденного» Министерства обороны Российской Федерации. EDN IUBQKF.
3. Использование технологий блокчейн для обеспечения информационной безопасности / В. А. Задбоев, В. Д. Шевяков, М. Д. Беседин, В. Е. Садовников // Современные тенденции развития фундаментальных и прикладных наук : Материалы VIII Всероссийской научно-практической конференции, Брянск, 25 января 2025 года. Брянск: Брянский государственный инженерно-технологический университет, 2025. С. 529–532. EDN VAKRLK.
4. Анализ проблем развития технологий блокчейн для обеспечения информационной безопасности в России / Д. Ю. Изотов, В. А. Задбоев, В. Д. Шевяков, В. Е. Садовников // Современные тенденции развития фундаментальных и прикладных наук : Материалы VIII Всероссийской научно-практической конференции, Брянск, 25 января 2025 года. Брянск: Брянский государственный инженерно-технологический университет, 2025. С. 532–536. EDN GSARHE.
5. Беседин, М. Д. анализ принципов работы DNS-серверов и DDoS-атак / М. Д. Беседин, В. А. Задбоев, В. Р. Полищук // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2024) : Материалы XIII Международной научно-технической и научно-методической конференции, Санкт-Петербург, 27–28 февраля 2024 года. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2024. С. 108–112. EDN LREHBE.

УДК 004.056

#### ОСОБЕННОСТИ МАНДАТНОГО КОНТРОЛЯ ЦЕЛОСТНОСТИ В ОПЕРАЦИОННОЙ СИСТЕМЕ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ ASTRA LINUX SPECIAL EDITION

Гребенников Тимофей Алексеевич

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mail: brabiner2.0@mail.ru

**Аннотация.** Операционная система специального назначения Astra Linux Special Edition создана для эксплуатации в условиях повышенных требований к защите информации. Одним из ключевых элементов её архитектуры безопасности является мандатный контроль целостности, обеспечивающий предотвращение несанкционированного воздействия на критически важные объекты системы. В работе рассмотрены принципы реализации механизма, его роль в общей модели безопасности, а также проведено сопоставление с подходами, применяемыми в системах SELinux и AppArmor. Особое внимание уделяется интеграции механизма в формализованную модель доступа, что обеспечивает предсказуемое поведение и формальную верификацию политик безопасности.

**Ключевые слова:** Astra Linux Special Edition; информационная безопасность; мандатный контроль целостности; модель безопасности; SELinux; AppArmor.

#### FEATURES OF MANDATORY INTEGRITY CONTROL IN THE ASTRA LINUX SPECIAL EDITION SPECIAL-PURPOSE OPERATING SYSTEM

Grebennikov Timofey

The Bonch-Bruevich Saint Petersburg State University of Telecommunications  
22 Bolshhevikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mail: brabiner2.0@mail.ru

**Abstract.** The special-purpose operating system Astra Linux Special Edition is designed for use in environments with stringent information security requirements. One of the key elements of its security architecture is mandatory integrity control, which prevents unauthorized access to critical system objects. This paper examines the implementation principles of this mechanism, its role in the overall security model, and compares it with approaches used in SELinux and AppArmor systems. Particular attention is paid to integrating this mechanism into a formalized access model, ensuring predictable behavior and formal verification of security policies.

**Keywords:** Astra Linux Special Edition; information security; mandatory integrity control; security model; SELinux; AppArmor.

Растущая сложность информационных систем и возрастающий спектр угроз делают актуальной задачу защиты критически важных компонентов операционных систем. Для государственных и военных структур, а также объектов критической инфраструктуры необходимы решения, гарантирующие строгий контроль целостности и исключение возможности скрытого воздействия на ядро и системные службы. Astra Linux Special Edition реализует такую возможность за счёт применения мандатного контроля целостности (МКЦ).

Принцип действия МКЦ заключается в присвоении субъектам и объектам системы уровней целостности. Субъект может модифицировать объект только в том случае, если его уровень целостности не ниже уровня целостности объекта [1]. Это исключает влияние менее доверенных процессов на более критичные ресурсы. Данный механизм становится особенно значимым при отражении атак, связанных с эксплуатацией уязвимостей в пользовательских приложениях, когда злоумышленник получает возможность запускать код от имени непривилегированного пользователя, администратора или суперпользователя, но лишается доступа к воздействию на высокоцелостные системные компоненты [2].

В отличие от SELinux, реализующего контроль доступа на основе концепции type enforcement, и AppArmor, использующего профили доступа, Astra Linux Special Edition интегрирует механизм контроля целостности в единую формализованную сущностно-ролевую модель управления доступом и информационными потоками [3–4]. Такая интеграция позволяет устранить конфликты между политиками и обеспечивает предсказуемое поведение системы при одновременной работе нескольких механизмов защиты. Кроме того, модель верифицируется методами формальной проверки, что повышает уровень доверия к её корректности [1].

Практическое значение внедрения МКЦ проявляется в возможности значительно снизить риск успешной реализации атак типа «повышение привилегий», «эскалация доступа» и «подмена системных файлов».

Сравнение с распространёнными в дистрибутивах Linux решениями показывает, что SELinux и AppArmor ограничиваются разграничением доступа и не предоставляют встроенного контроля целостности. Это делает Astra Linux Special Edition уникальной в своём классе и обеспечивает её преимущество при использовании в системах, где требуется высокая степень гарантированной защиты.

Таким образом, мандатный контроль целостности в Astra Linux Special Edition является ключевым элементом многоуровневой архитектуры безопасности, формирующим основу для доверенного функционирования системы. Его интеграция с ролевым и мандатным управлением доступом обеспечивает комплексный подход к защите информации и делает данное решение приоритетным для использования в государственных и оборонных информационных системах.

#### СПИСОК ЛИТЕРАТУРЫ

1. Девянин П. Н., Кулямин В. В., Петренко А. К., Хорошилов А. В., Щепетков И. В. Интеграция мандатного и ролевого управления доступом и мандатного контроля целостности в верифицированной иерархической модели безопасности операционной системы // Труды ИСП РАН. 2020. №1. С. 7-26.
2. Буренин П. В., Девянин П. Н., Лебеденко Е. В., Проскурин В. Г., Цибуля А. Н. Безопасность операционной системы специального назначения Astra Linux Special Edition М.: Горячая линия Телеком, 2019, 404 с.
3. Вермейлен С. Администрирование системы защиты SELinux / пер. с англ. Верецагина В. Л., Севостьянова О. К. М.: ДМК Пресс, 2020, 300 с.
4. Тиволт Д. Защита и укрепление Linux / пер. с англ. Слинкин А. М.: ДМК-Пресс, 2023, 618 с.

УДК 004.056

#### УГРОЗЫ И МЕТОДЫ ЗАЩИТЫ ОТ АТАК ОТРАВЛЕНИЯ ДАННЫХ В СИСТЕМАХ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Гугунишвили Лали Джумберовна<sup>1</sup>, Живодовский Иван Иванович<sup>2</sup>, Шулындина Мария Сергеевна<sup>1</sup>

<sup>1</sup> Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

<sup>2</sup> Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: guginashvili3343@gmail.ru, ivan.zhivodovsky32@mail.ru, mashash300102@gmail.com

**Аннотация.** Актуальность темы защиты моделей машинного обучения от атак отправления данных обусловлена быстрым ростом их применения в различных сферах жизни. Искусственный интеллект все чаще используется в критически важных областях, таких как медицина, финансы, транспорт и безопасность, где от точности и надежности решений зависит безопасность и благополучие людей. В условиях активного использования больших данных и открытых источников существует высокий риск внедрения вредоносных

образцов, способных искажать результаты работы систем и приводить к ошибочным выводам. Поэтому разработка методов обнаружения и предотвращения атак отравления данными становится важнейшей задачей для обеспечения устойчивости и доверия к ИИ-технологиям.

**Ключевые слова:** машинное обучение; алгоритмы защиты; безопасность ИИ; атаки отравления данными; устойчивость моделей.

## THREATS AND METHODS OF PROTECTION AGAINST DATA POISONING ATTACKS IN ARTIFICIAL INTELLIGENCE SYSTEMS

Guginashvili Lali<sup>1</sup>, Zhivodovsky Ivan<sup>2</sup>, Shulyndina Maria<sup>1</sup>

<sup>1</sup> The Bonch-Bruевич Saint Petersburg State University of Telecommunications  
22 Bolshhevikov Av, bldg 1, St. Petersburg, 193232, Russia

<sup>2</sup> The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny  
3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: guginashvili3343@gmail.ru, ivan.zhivodovsky32@mail.ru, mashash300102@gmail.com

**Abstract.** The relevance of the topic of protecting machine learning models from data transmission attacks is due to the rapid growth of their use in various spheres of life. Artificial intelligence is increasingly being used in critical areas such as medicine, finance, transportation, and security, where the safety and well-being of people depend on the accuracy and reliability of solutions. In conditions of active use of big data and open sources, there is a high risk of introducing malicious samples that can distort the results of systems and lead to erroneous conclusions. Therefore, the development of methods for detecting and preventing data transmission attacks is becoming an essential task to ensure the sustainability and trust in AI technologies.

**Keywords:** machine learning; protection algorithms; AI security; data poisoning attacks; model stability.

Атаки отравления данными представляют собой целенаправленные злоумышленные воздействия, при которых злоумышленники внедряют специально созданные вредоносные образцы в обучающую выборку [1]. Цель таких атак — изменить поведение модели, вызвать неправильную классификацию или открыть скрытые уязвимости, такие как бэкдоры. Эти атаки могут осуществляться с минимальными затратами и без необходимости знания внутренней архитектуры системы, что делает их особенно опасными в условиях открытых и распределенных систем обучения. В связи с этим актуальность разработки методов обнаружения и защиты от подобных угроз становится критической для обеспечения безопасности и надежности современных систем искусственного интеллекта [2].

В области атак на модели машинного обучения выделяют несколько ключевых типов, каждый из которых обладает своими особенностями и методами реализации. Эти атаки направлены на нарушение работы системы, получение нежелательной информации или создание условий для неправильных выводов модели [3].

### 1. Вредоносные образцы (Poisoning Attacks).

Данный тип атак предполагает внедрение специально подготовленных данных в обучающую выборку с целью искажения процесса обучения или поведения модели. В результате модель учится неправильно классифицировать определённые образцы или демонстрировать нежелательные реакции. Виды вредоносных образцов включают:

- ядовитое обучение (Data Poisoning) — злоумышленник добавляет или изменяет данные в обучающем наборе, чтобы вызвать ошибочные предсказания или ослабить модель;
- отравление тестовых данных (Test-time Poisoning) — внедрение вредоносных образцов в тестовую выборку, чтобы сбить с толку модель во время её использования.

### 2. Атаки с использованием скрытых уязвимостей (Backdoor Attacks) [4].

Модель обучается так, чтобы при появлении определённого триггера (например, специфического паттерна или изображения) она демонстрировала нежелательное поведение. Такой триггер обычно невидим или трудно обнаружим, что делает атаку особенно опасной. В результате злоумышленник может активировать скрытую «заднюю дверь» в модели, вызывая неправильные выводы по заданным условиям.

### 3. Атаки на доверие модели (Model Stealing / Model Extraction).

Злоумышленник пытается получить полное или частичное понимание внутренней структуры или параметров модели, обращаясь к ней с большим количеством запросов. Это позволяет копировать модель, создавать её аналоги или выявлять уязвимости, не имея прямого доступа к исходному коду или данным [5].

### 4. Атаки с использованием adversarial examples (Adversarial Attacks).

Это создание небольших, зачастую неотличимых от оригинала, изменений входных данных, которые вызывают неправильную работу модели. Например, небольшие искажения на изображении могут заставить систему распознавать его как что-то другое. Такие атаки особенно актуальны в задачах компьютерного зрения и голосового распознавания.

### 5. Атаки обхода (Evasion Attacks).

Нацелены на обход систем защиты или фильтров после обучения модели. Злоумышленник использует специально подготовленные образцы, чтобы пройти через системы защиты и добиться нежелательных результатов без вмешательства в обучение [6].



Условия успешности атак: необходимость доступа к данным или этапу обучения, знание архитектуры модели, даже 1–3% отравленных данных могут существенно навредить.

Современные методы защиты от атак отравления данных включают проверку источников и автоматическую фильтрацию подозрительных образцов. Также используют устойчивые алгоритмы обучения, которые снижают влияние аномальных данных, и принципы дифференциальной приватности, усложняющие целенаправленные атаки [7]. Важна проверка модели с помощью аудитов для выявления скрытых уязвимостей, а также методы очистки данных — кластеризация и поиск аномалий. Например, использование PCA и алгоритма DBSCAN помогает выявить и удалить вредоносные образцы, группируя похожие и отмечая выбросы. Эти меры повышают надежность ИИ и снижают риск внедрения вредоносных данных [8].

В эксперименте на датасете MNIST внедрили триггер — белый квадрат на цифре «7», и изменили её метку на «1». Модель обучили на такой искажённой выборке, и она ошибочно распознавала «7 с триггером» как «1». Для защиты использовали PCA для снижения признаков и алгоритм DBSCAN для кластеризации [9]. Образы, не входящие в кластеры, считались аномалиями и удалялись. После фильтрации модель стала менее уязвимой к атаке. Этот опыт подтвердил эффективность автоматических методов обнаружения и устранения вредоносных данных, особенно при работе с открытыми источниками.

Даже небольшие вмешательства в данные могут значительно исказить работу модели. Использование методов кластеризации помогает выявить и устранить потенциально вредоносные примеры. Выводы:

- атаки отравления — скрытая, но очень опасная угроза для ИИ, особенно в ответственных сферах;
- эффективная защита требует комплексного подхода: контроль качества данных, устойчивые алгоритмы, автоматическая фильтрация и регулярные аудиты;
- внедрение прозрачности и интерпретируемости решений помогает снизить риски;
- необходимость развития адаптивных и автоматизированных защитных механизмов для повышения устойчивости систем.

Обеспечение безопасности ИИ-систем при использовании открытых данных и автоматизированных ML-процессов требует системного подхода, включающего профилактику, мониторинг и оперативное реагирование на угрозы. Внедрение методов фильтрации, кластеризации и анализа признаков — важные инструменты для повышения надёжности и доверия к современным моделям машинного обучения [10].

#### СПИСОК ЛИТЕРАТУРЫ

1. Красов А. В., Левин М. В., Штеренберг С. И., Исаченков П. А. Модель управления потоками трафика в программно-определяемой сети с изменяющейся нагрузкой // Научные технологии в космических исследованиях Земли. 2016. Т. 8, № 4. С. 70–74. EDN WNEHJT.
2. Живодовский И. И. Машинное обучение в прогнозировании потребности материально-технического обеспечения войск: анализ существующих решений и перспективная модель // Проблемы технического обеспечения войск в современных условиях : Труды X Межвузовской научно-практической конференции, СПб, 16 мая 2025 года. СПб : ФГКВОУ ВО «Военная академия связи им. Маршала Советского Союза С. М. Буденного» МО РФ, 2025. С. 107–111. EDN YNNIXT.
3. Красов А. В., Косов Н. А., Холоденко В. Ю. Исследование методов провижининга безопасной сети на мультивендорном оборудовании с использованием средств автоматизированной конфигурации // Colloquium-Journal. 2019. № 13-2(37). С. 243–247. EDN MJVGAY.
4. Тран Б., Ли Ю., Атрэн Б. Спектральные сигнатуры в backdoor-атаках // Advances in Neural Information Processing Systems. 2018. Т. 31. С. 8000–8010.
5. Ханина А. И., Бобровский И. А. Методы противодействия угрозам безопасности в машинном обучении // Информационная безопасность. 2021. № 2. С. 23–30.
6. Шевченко А. А. Модель процесса защиты информационно-телекоммуникационной сети от несанкционированного воздействия // Инновационная деятельность в Вооруженных Силах Российской Федерации : Труды всеармейской научно-практической конференции, СПб, 10–11 октября 2019 года. СПб : Военная академия связи им. Маршала Советского Союза С. М. Буденного» МО РФ, 2019. С. 166–173.
7. Билятинов К. З., Красов А. В., Меняйло В. В. Исследование систем и анализ результатов испытаний. СПб : Центр научно-информационных технологий «Астерион», 2019. 362 с. ISBN 978-5-00045-813-6. EDN OXKBZW.
8. Леонов, Ю. А., Филиппов Р. А., Живодовский И. И. Использование методов обработки естественного языка в формировании рейтинговой системы высших учебных заведений РФ // Известия Тульского государственного университета. Технические науки. 2024. № 2. С. 20–28. DOI 10.24412/2071-6168-2024-2-20-21. EDN FSZWDR.
9. Тищенко А. А., Живодовский И. И. Разработка программного модуля для определения тональности отзывов о высших учебных заведениях РФ // Автоматизация и моделирование в проектировании и управлении : сборник научных статей Всероссийской конференции, Брянск, 22 мая 2023 года. Курс : ЗАО «Университетская книга», 2023. С. 193–196. EDN IOYOU.
10. Липатников В. А., Парфиров В. А., Шевченко А. А., Мелехов К. В. Модель процесса обеспечения безопасности сети передачи данных в условиях информационного противоборства // Актуальные проблемы защиты и безопасности : Труды XXVI Всероссийской научно-практической конференции, СПб, 03–06 апреля 2023 года. Том 1. СПб : Типография Любавич, 2023. С. 569–572.

УДК 004.056

#### NRD-СПИСКИ КАК КОМПОНЕНТ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

**Гудаков Антон Павлович, Миняев Андрей Анатольевич, Скорых Марк Андреевич**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Большевикова пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

e-mails: real1905@mail.ru, minyaev.a@gmail.com, mark.skorykh@bk.ru

**Аннотация.** В докладе рассматриваются NRD-списки в качестве дополнительного источника сведений для эксплуатации средств защиты информации. Были проанализированы статьи и исследования, которые

позволяют определить перечень решений, которые можно дополнить информацией о недавно зарегистрированных доменах.

**Ключевые слова:** NRD; DNS; защита; безопасность; защита информации.

## NRD-LISTS AS A COMPONENT OF INFORMATION SECURITY SOLUTIONS

**Gudakov Anton, Minyaev Andrey, Skorykh Mark**

The Bonch-Bruевич Saint Petersburg State University of Telecommunications

22 Bolshhevikov Av, bldg 1, St. Petersburg, 193232, Russia

e-mails: reall905@mail.ru, minyaev.a@gmail.com, mark.skorykh@bk.ru

**Abstract.** The article examines NRD-lists as an additional source of information for exploiting information security tools. Articles and studies were analyzed to determine a list of solutions that can be supplemented with information about newly registered domains.

**Keywords:** NRD; DNS; protection; security; information protection.

В современном мире тяжело представить компанию, которая пользовалась бы исключительно собственным программным обеспечением или покупала его только у одного вендора. Для разных задач могут использоваться приложения от независимых поставщиков. Кибератаки с течением времени развиваются, а атакующие начали использовать особенность с использованием чужого программного обеспечения в своих целях [1]. Так, например, появились атаки на цепочки поставок. В рамках их реализации вредоносному воздействию подвергается продукт или услуга, которые предоставляется другим компаниям.

Появление данной тенденции привело к тому, что взаимодействие с поставщиками и заказчиками стали стараться сильнее обезопасить. Также это привело к возникновению идеи о выработке коллективного подхода к защите информации. Одним из способов его обеспечения можно назвать ведение общедоступных баз знаний, содержащих в себе сведения об активах злоумышленников. К ним относят IP-адреса, hash-суммы и доменные имена. Их и некоторые другие свойства активов прозвали индикаторами компрометации (IOC).

NRD-списки (Newly Registered Domain lists) предоставляют информацию о недавно зарегистрированных доменных именах. Если верить исследованиям Palo Alto [2], Forbes [3], Stamus Networks [4] и WhoAPI [5], эти активы представляют определенные риски информационной безопасности. Это могут мошеннические ресурсы, фишинговые сайты и сервера для распространения вредоносного программного обеспечения. Блокировать все доменные имена из этих списков не желательно, поскольку в необходимый момент можно не получить доступ к только что созданному демонстрационному стенду, новому легитимному сервису или иному безопасному контенту. NRD-списки это инструмент, которым необходимо пользоваться с умом.

Первым, что приходит на ум — использование списков недавно зарегистрированных доменов в качестве помощи при проведении расследований инцидентов информационной безопасности или поиска следов компрометации системы. Интеграция с IDS/IPS (Intrusion Detection System/Intrusion Prevention System) позволит быстро выявлять подозрительную активность в сети. Наличие активов из NRD-списков в трафике не всегда будет указывать на вредоносное воздействие, однако информация о них может значительно сократить время, необходимое на реагирование на инцидент.

Обогащение событий из SIEM-систем (Security Information and Event Management) упростит работу аналитиков информационной безопасности. Создание предупреждений о появлении активности, связанной с NRD-списками, расширит возможности мониторинга и сократит время, необходимое на обнаружение злоумышленников.

YARA-сканеры также могут использовать информацию из списков недавно зарегистрированных доменов для поиска вредоносных файлов, в которых содержатся строки с вредоносными активами. Такой подход может помочь при исследовании устройства обнаружить экземпляры опасного программного обеспечения.

Таким образом, NRD-списки можно использовать совместно с различными средствами защиты информации с целью обнаружения потенциально вредоносной активности. Основной упор делается на исследование сетевого трафика или взаимодействия приложений, в рамках которых используются доменные имена. Помимо этого, можно использовать сведения оттуда и при анализе различных файлов, для выявления возможных вредоносных функций.

## СПИСОК ЛИТЕРАТУРЫ

1. Актуальные киберугрозы: IV квартал 2024 года — I квартал 2025 года // Positive Technologies. [Электронный ресурс]. URL: <https://ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iv-kvartal-2024-goda-i-kvartal-2025-goda/#id21> (дата обращения: 02.07.2025).
2. What Are Malicious Newly Registered Domains? // Paloalto networks. [Электронный ресурс]. URL: <https://www.paloaltonetworks.com/cyberpedia/what-are-malicious-newly-registered-domains> (дата обращения: 01.07.2025).
3. Newly Registered Domains: To Block Or Not To Block? // Forbes. [Электронный ресурс]. URL: <https://www.forbes.com/councils/forbestechcouncil/2024/10/25/newly-registered-domains-to-block-or-not-to-block> (дата обращения: 02.07.2025).
4. Introducing Open NRD: Newly Registered Domain Threat Intel Feeds for Suricata // Stamus Networks. [Электронный ресурс]. URL: <https://www.stamus-networks.com/blog/introducing-open-nrd> (дата обращения: 02.07.2025).
5. Cybersecurity Implications Around Newly Registered Domains // WhoAPI. [Электронный ресурс]. URL: [https://whoapi.com/blog/why-are-newly-registered-domains-important-for-cybersecurity/#Malicious\\_Use\\_of\\_Newly\\_Registered\\_Domains](https://whoapi.com/blog/why-are-newly-registered-domains-important-for-cybersecurity/#Malicious_Use_of_Newly_Registered_Domains) (дата обращения: 02.07.2025).

УДК 004.056

## ЗАЩИТА ИНФОРМАЦИОННЫХ СИСТЕМ ОТ СЕТЕВОЙ РАЗВЕДКИ МЕТОДАМИ АНАЛИЗА ТРАФИКА

Дзиговский Владислав Андреевич<sup>1</sup>, Живодовский Иван Иванович<sup>2</sup>, Шадрин Илья Дмитриевич<sup>1</sup>

<sup>1</sup> Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевикова пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

<sup>2</sup> Военная академия связи им. Маршала Советского Союза С. М. Буденного  
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: dzigovskii.va@sut.ru, ivan.zhivodovsky32@mail.ru, shadrin.ilya.96@mail.ru

**Аннотация.** Данная статья посвящена классификации методов обнаружения сетевого сканирования и способов обеспечения безопасности информационных систем. В ней детально разбираются методики идентификации подозрительного трафика, такие как сигнатурный, статистический и поведенческий анализ, а также алгоритмы машинного обучения. Важным аспектом является отделение злонамеренной активности от фоновой за счет исследования временных меток, видов пакетов и IP-адресов, что ведет к улучшению работы систем защиты.

**Ключевые слова:** кибербезопасность; информационная безопасность; зондирование сети; вредоносная активность; мониторинг сети; сетевой трафик; сегментация сети; пентест.

## PROTECTION OF INFORMATION SYSTEMS FROM NETWORK INTELLIGENCE BY TRAFFIC ANALYSIS METHODS

Dzigovskii Vladislav<sup>1</sup>, Zhivodovsky Ivan<sup>2</sup>, Shadrin Ilya<sup>1</sup>

<sup>1</sup> The Bonch-Bruевич Saint Petersburg State University of Telecommunications  
22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia

<sup>2</sup> Military Academy of Communications named after S. M. Budyonny.  
3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: dzigovskii.va@sut.ru, ivan.zhivodovsky32@mail.ru, shadrin.ilya.96@mail.ru

**Abstract.** This article is devoted to the classification of network scanning detection methods and ways to ensure the security of information systems. It explains in detail the methods of identifying suspicious traffic, such as signature, statistical and behavioral analysis, as well as machine learning algorithms. An important aspect is to separate malicious activity from the background by examining timestamps, packet types, and IP addresses, which leads to improved security systems.

**Keywords:** cybersecurity; information security; network sensing; malicious activity; network monitoring; network traffic; network segmentation; pentest.

Сетевое сканирование — это ключевой этап подготовки кибератак, используемый злоумышленниками для обнаружения уязвимостей и активных узлов в атакуемой сети. Методы сетевой разведки позволяют получить скрытые данные о топологии сети и конфигурации устройств [1].

Целью данной работы является систематизация современных методов детектирования таких сканирований, анализа для аномального и легитимного трафика, а также обзор стратегий защиты информационных инфраструктур.

Следовательно, настоящее исследование направлено на решение злободневной задачи, порождённой современными вызовами кибербезопасности, такими как распространение зашифрованного трафика и распределённые атаки.

Эффективное выявление сетевого сканирования, учитывающее многообразие методов зондирования и сложность различения вредоносной и фоновой активности, требует применения комплексных мер [2].

В качестве ключевых можно выделить следующие подходы:

- сигнатурный анализ, основанный на сопоставлении данных с эталонными шаблонами аномалий (классический пример — flood SYN-пакетов без установления соединения);
- статистический анализ, который идентифицирует отклонения от базовых показателей трафика (аномальная активность узла, сканирование портов, повышенное число неудачных подключений) [3];
- поведенческий анализ, заключающийся в моделировании нормального сетевого поведения и детектировании отклонений от профиля;
- методы машинного обучения (в т.ч. классификация и кластеризация), обеспечивающие гибкость и адаптивность систем обнаружения к эволюции угроз.

Принципиальная трудность заключается в надёжном разграничении сканирующей активности и легитимных сетевых процессов, к которым относятся, в частности, обновление программного обеспечения и синхронизация данных с облачными сервисами [4, 5].

Решение данной задачи обеспечивается за счёт применения временных и контекстных фильтров, исследования типов пакетов (например, преобладание SYN-пакетов без ответных ACK или сообщения ICMP Unreachable), а также использования поведенческих баз данных, фиксирующих историю взаимодействия узлов.

В контексте увеличения доли зашифрованного трафика и распространения распределённых атак (таких как медленное сканирование), повышенную значимость приобретает анализ метаданных — частоты, объёма и

направленности сетевых запросов. Для обработки этой информации в режиме реального времени используются такие инструменты, как Wireshark, Zeek и Elastic Stack [6–9].

Повышение эффективности детектирования сетевого сканирования достигается за счёт интеграции систем наблюдения со средствами автоматического противодействия. В качестве практических мер можно выделить:

- развёртывание honeypots с целью дезориентации злоумышленников и детального изучения их методов;
- реализацию динамической фильтрации сетевого потока на основе правил межсетевых экранов и систем обнаружения/предотвращения вторжений (IDS/IPS);
- внедрение SIEM-платформ, обеспечивающих корреляцию событий безопасности и формирование целостной картины инцидентов.

Следовательно, нейтрализация угроз, связанных с сетевым сканированием, основывается на многоуровневой стратегии, сочетающей в себе анализ данных, фильтрацию трафика, визуализацию и автоматическое реагирование. Максимальная эффективность защиты возможна лишь при комплексном использовании технологий, своевременном обновлении сигнатур и грамотной конфигурации всех компонентов.

#### СПИСОК ЛИТЕРАТУРЫ

1. Бредихин С.В., Костин В.И., Щербакова Н. Г. Обнаружение сканеров в IP-сетях методом последовательного статистического анализа // Вестник НГУ. Сер: Информационные технологии. 2009. № 4. URL: <https://cyberleninka.ru/article/n/obnaruzhenie-skanerov-v-ip-setyah-metodom-posledovatel'nogo-statisticheskogo-analiza> (дата обращения: 10.05.2025).
2. Колесников, А. А. Особенности реагирования на атаки типа «сканирование сетевых портов» средствами управления инцидентами информационной безопасности thehive / А. А. Колесников, И. М. Шендеевич // Актуальные проблемы инфотелекоммуникаций в науке и образовании : Сборник научных статей XIII Международной научно-технической и научно-методической конференции в 4 т., Санкт-Петербург, 27–28 февраля 2024 года. Санкт-Петербург: СПбГУ телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2024. С. 454-459.
3. Ушаков, И. А. Методика обнаружения аномалий в сетевом трафике с использованием IPS на основе Security Onion / И. А. Ушаков, А. В. Красов, Д. Д. у. Мулладжанов // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2022. № 1. С. 5-11.
4. Гетьман, А. И. Обзор методов классификации сетевого трафика с использованием машинного обучения / А. И. Гетьман, М. К. Иконникова // Труды Института системного программирования РАН. 2020. Т. 32, № 6. С. 137-154.
5. Шевченко А. А. Модель процесса защиты информационно-телекоммуникационной сети от несанкционированного воздействия // Инновационная деятельность в Вооруженных Силах Российской Федерации: Труды всеармейской научно-практической конференции, Санкт-Петербург, 10–11 октября 2019 года. СПб: ФГКВУ ВО Военная академия связи им. Маршала Советского Союза С.М. Буденного» МО РФ, 2019. С. 166-173.
6. Липатников В.А., Парфилов В.А., Шевченко А.А., Мелехов К.В. Модель процесса обеспечения безопасности сети передачи данных в условиях информационного противоборства // Актуальные проблемы защиты и безопасности: Труды XXVI Всероссийской научно-практической конференции, Санкт-Петербург, 03–06 апреля 2023 года. Том 1. Санкт-Петербург: Типография Любавич, 2023. С. 569-572.
7. Липатников В.А., Шевченко А.А., Омаров Р.Г. Способ защиты информационных сетей транспортных систем от DDoS-атак с прогнозированием // Транспорт России: проблемы и перспективы 2019: Материалы международной-научно-практической конференции, Санкт-Петербург, 12–13 ноября 2019 года. Т. 1. СПб: Институт проблем транспорта им. Н.С. Соломенко РАН, 2019. С. 413-417.
8. Методология управления потоками трафика в программно-определяемой адаптивной сети / А. В. Красов, М. В. Левин, С. И. Штеренберг, П. А. Исаченков // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2016. № 4. С. 3-8.
9. Исаченков, П. А. Исследование эффективности метода управления потоками трафика на основе информации о нагрузке в программно-определяемой сети с неравными метриками маршрутов / П. А. Исаченков, А. В. Красов, М. В. Левин // Современная наука и инновации. 2017. № 2(18). С. 32-38.

УДК 004.056.5

#### ZVIRT КАК ЗАЩИЩЁННОЕ СРЕДСТВО ВИРТУАЛИЗАЦИИ

**Дюсметова Азалия Айдаровна, Пестов Игорь Евгеньевич, Алексеева Ксения Евгеньевна**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

Большевиков, пр., 22, корп.1, Санкт-Петербург, 193232, Россия

e-mails: [dyusmetova\\_azaliya@mail.ru](mailto:dyusmetova_azaliya@mail.ru), [pestov.ie@sut.ru](mailto:pestov.ie@sut.ru), [ksenya.alekseeva523@mail.ru](mailto:ksenya.alekseeva523@mail.ru)

**Аннотация.** Результаты анализа показывают, что при корректной настройке и соблюдении рекомендаций по изоляции сетей, ограничению сервисов и контролю доступа, zVirt может рассматриваться как защищённое средство виртуализации, соответствующее современным требованиям информационной безопасности.

**Ключевые слова:** администрирование; безопасность; виртуализация; zVirt; система аутентификации и авторизации.

#### ZVIRT AS A SECURE VIRTUALIZATION PLATFORM

**Dyusmetova Azaliya, Pestov Igor, Alekseeva Kseniya**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia

e-mails: [dyusmetova\\_azaliya@mail.ru](mailto:dyusmetova_azaliya@mail.ru), [pestov.ie@sut.ru](mailto:pestov.ie@sut.ru), [ksenya.alekseeva523@mail.ru](mailto:ksenya.alekseeva523@mail.ru)

**Abstract.** The results of the analysis demonstrate that, with proper configuration and adherence to recommendations on network isolation, service limitation, and access control, zVirt can be regarded as a secure virtualization platform that meets modern information security requirements.

**Keywords:** administration; security; virtualization; zVirt; authentication and authorization system.

Современные ИТ-инфраструктуры активно используют виртуализацию для оптимизации ресурсов, повышения отказоустойчивости и упрощения управления вычислительными мощностями. Однако рост числа виртуальных систем сопровождается увеличением числа угроз, связанных с кибератаками.

Предлагается рассмотреть проблему обеспечения информационной безопасности в средах виртуализации на примере платформы zVirt — отечественная платформа, основанная на проекте oVirt и доработанная в соответствии с российскими стандартами информационной безопасности.

Среди ключевых преимуществ платформы zVirt следует выделить её адаптацию к требованиям отечественных регуляторов и специфике функционирования критической информационной инфраструктуры. Получение сертификата соответствия ФСТЭК подтверждает возможность применения системы в средах с повышенными требованиями к уровню доверия и безопасности, включая государственные информационные системы, объекты промышленности и энергетики, а также финансовый сектор [1–3].

В основе zVirt лежит гипервизор KVM, встроенный в ядро Linux и поддерживающий аппаратную виртуализацию на современных процессорах. Система предусматривает возможность кластеризации гипервизоров, что обеспечивает функции высокой доступности и живой миграции виртуальных машин, а также использует сетевую сегментацию на основе VLAN, что позволяет изолировать управляющий и пользовательский трафик [4].

Важное значение для безопасности zVirt имеет встроенная поддержка систем аутентификации и авторизации: LDAP, Active Directory, FreeIPA [5]. При корректной настройке администраторы могут централизованно управлять доступом и контролировать учётные записи. Кроме того, управление виртуальной инфраструктурой осуществляется через веб-консоль, что повышает удобство, но одновременно требует защиты управляющей сети, которая должна быть вынесена в отдельный сегмент.

Тем не менее, как и в любой системе, потенциальные риски связаны с конфигурацией и администрированием. Возможность установки пакетов без проверки цифровой подписи, избыточные сервисы на гипервизорах, а также уязвимости SSH-сессий могут быть использованы злоумышленниками. Однако эти угрозы устраняются за счёт правильных мер: отключения ненужных сервисов, шифрования дисков виртуальных машин, изоляции управляющих сетей и применения строгих политик аутентификации.

zVirt при корректной настройке и эксплуатации может рассматриваться как надёжное средство виртуализации, отвечающее современным требованиям безопасности. Архитектура системы предоставляет все необходимые инструменты для минимизации поверхности атаки, а эффективность защиты определяется качеством администрирования и соблюдением рекомендаций по информационной безопасности.

#### СПИСОК ЛИТЕРАТУРЫ

1. Печенкина А. В., Селифанов В. В. Системы обеспечения безопасности, применяемые при использовании технологии виртуализации // Интерэкспо Гео-Сибирь 2019 №2 т.19
2. Силаков Д. В. Использование аппаратной виртуализации в контексте информационной безопасности // Труды Института системного программирования РАН 2011. т. 20
3. Терещенко Г. В., Новикова Ю. А. Использование виртуализации на ПК СВ «Брест» для обучения методам информационной безопасности // Инженерный вестник Дона 2023. № 12.
4. Красов А.В., Штеренберг С.И., Москальчук А.И. Методология создания виртуальной лаборатории для тестирования безопасности распределенных информационных систем // Вестник Рязанского Государственного Технического Университета 2020. N 3(88). С. 38-46.
5. Денисов В. Д. Установка и настройка лабораторного стенда на базе proxmox ve и системы wazuh для оценки защищенности информационных систем // Вестник науки 2025 №6, С. 1675-1679.

УДК 004.056

#### АДАПТАЦИЯ МЕТОДОЛОГИИ ЗАЩИЩЁННОЙ РАЗРАБОТКИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ ДЛЯ КОМАНД РАЗНОГО МАСШТАБА

**Емельянов Николай Романович, Ковцур Максим Михайлович**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mails: kolaemelanov60@gmail.com, Maxkovzur@mail.ru

**Аннотация.** В работе рассматривается методология sMADLC (Security-aware Mobile Application Development Lifecycle) и предлагается её адаптация к условиям команд разного масштаба. Подход предполагает разделение на полноценный вариант, ориентированный на средние и крупные компании, и упрощённый вариант (sMADLC-lite), позволяющий малым командам интегрировать практики проектирования с учётом безопасности без привлечения выделенных специалистов по информационной безопасности.

**Ключевые слова:** информационная безопасность; мобильные приложения; Secure by Design; SSDLC; sMADLC; sMADLC-lite.

#### ADAPTATION OF SECURE MOBILE APPLICATION DEVELOPMENT METHODOLOGY FOR TEAMS OF DIFFERENT SCALES

**Emelyanov Nikolai, Kovtsur Maxim**

The Bonch-Bruевич Saint Petersburg State University of Telecommunications  
22 Bolshhevikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mails: kolaemelanov60@gmail.com, Maxkovzur@mail.ru

**Abstract.** The study examines the sMADLC (Security-aware Mobile Application Development Lifecycle) methodology and proposes its adaptation to teams of different scales. The approach involves dividing into a full-featured version oriented towards medium and large companies, and a simplified version (sMADLC-lite) that allows small teams to integrate Secure by Design practices without involving dedicated information security specialists.

**Keywords:** information security; mobile applications; Secure by Design; SSDLC; sMADLC; sMADLC-lite.

Рост количества мобильных приложений и усложнение их функциональности приводят к увеличению поверхности атак и возрастанию рисков информационной безопасности.

Недавние эмпирические исследования показывают, что до 95% мобильных приложений не проходят хотя бы одну категорию OWASP MASVS, что указывает на значимый разрыв между практиками разработки и требованиями к защищенности [1].

Традиционные подходы к обеспечению безопасности, основанные на проверке готового продукта, не способны эффективно решать проблемы безопасности в контексте быстрой разработки мобильных приложений.

Данное исследование направлено на разработку методики, основанной на принципах sMADLC (Security-aware Mobile Application Development Lifecycle) [2]. В отличие от исходного подхода, рассчитанного на организации с выделенными ресурсами в области информационной безопасности, предлагаемая версия адаптирована для небольших команд.

Цель работы заключается в создании sMADLC-lite — упрощённого варианта, который сохраняет ключевые элементы обеспечения безопасности, но распределяет ответственность между членами команды и снижает организационные издержки.

Результаты исследований Kumar & Vithani [2], OWASP MASDG [3] и Shostack [4] показывают, что отдельные методы не покрывают весь жизненный цикл.

Моделирование угроз (STRIDE, DREAD) помогает выявлять риски, но не определяет процессы [5, 6]. Стандарты MASVS/MASTG оценивают продукт, но не обеспечивают встроенную защиту. Это подтверждает необходимость комбинированного подхода, реализованного в sMADLC-lite.

В заключение sMADLC-lite сохраняет критические элементы безопасности, снижает организационные издержки и обеспечивает плавный переход к полной методологии при росте ресурсов.

#### СПИСОК ЛИТЕРАТУРЫ

1. NowSecure. 95% of mobile apps fail the OWASP MASVS industry standard for mobile security, finds NowSecure Industry Benchmark. Электронный ресурс. Режим доступа: <https://www.nowsecure.com/press-releases/95-of-mobile-apps-fail-the-owasp-masvs-industry-standard-for-mobile-security-finds-nowsecure-industry-benchmark/> (дата обращения: 06.09.2025).
2. sMADLC: Security-aware Mobile Application Development Lifecycle. Электронный ресурс // International Journal of Education and Management Engineering. 2023. Т. 13. № 2. С. 39-49. Режим доступа: <https://www.mecspress.org/ijeme/ijeme-v13-n2/IJEME-V13-N2-5.pdf> (дата обращения: 06.09.2025).
3. OWASP Mobile Application Security News Archive 2024: MASVS, MASTG, MASWE. Электронный ресурс. OWASP Foundation, 2024. Режим доступа: <https://mas.owasp.org/news/archive/2024/> (дата обращения: 07.09.2025).
4. Shostack, Adam. The Ultimate Beginner's Guide to Threat Modeling. Электронный ресурс. Режим доступа: <https://shostack.org/resources/threat-modeling#why-so-many> (дата обращения: 08.09.2025).
5. Сравнение фреймворков STRIDE, DREAD и PASTA для моделирования угроз. Электронный ресурс. Режим доступа: <https://www.softwaresecured.com/post/comparison-of-stride-dread-pasta> (дата обращения: 09.09.2025).
6. Ковцур М. М. и др. Разработка защищенного мобильного приложения для Android // ПКМ-2024. СПбГУТ, 2025. С. 395-399.

УДК 004.051

#### ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ТУМАННЫХ ВЫЧИСЛЕНИЙ

Задбоев Вадим Александрович<sup>1</sup>, Зозуля Глеб Сергеевич<sup>2</sup>

<sup>1</sup> Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

<sup>2</sup> Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Большевикова пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

e-mails: zozulya.gleb@mail.ru, zadboev89@mail.ru

**Аннотация.** Рост числа устройств Интернета вещей (IoT) и объёмов генерируемых данных стимулирует развитие туманных вычислений (Fog computing), обеспечивающих обработку данных на периферии сети, снижение задержек и повышение эффективности. Однако децентрализованная, гетерогенная и ресурсоограниченная природа Fog-узлов создаёт новые вызовы в области безопасности, дополняя традиционные угрозы, характерные для облачных систем, такими как утечки данных и нарушения конфиденциальности. В данной работе представлен всесторонний обзор методов обеспечения безопасности в сетях туманных вычислений с акцентом на эталонную архитектуру OpenFog. Рассматриваются ключевые уязвимости, угрозы и современные подходы к защите, включая аутентификацию, шифрование, управление доступом и мониторинг.

**Ключевые слова:** fog computing; безопасность; OpenFog.

## ENSURING INFORMATION SECURITY BASED ON FOG COMPUTING

Zozulya Gleb<sup>1</sup>, Shevchenko Aleksandr<sup>1</sup>

<sup>1</sup> The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny  
3 Tikhoretsky Av, St. Petersburg, 194064, Russia

<sup>2</sup> The Bonch-Bruевич Saint Petersburg State University of Telecommunications  
22 Bolshhevikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mails: zozulya.gleb@mail.ru, zadboev89@mail.ru

**Abstract.** The growth of the Internet of Things (IoT) devices and the volume of data generated is driving the development of fog computing, which enables data processing at the network edge, reducing latency and increasing efficiency. However, the decentralized, heterogeneous and resource-constrained nature of fog nodes creates new security challenges, in addition to traditional threats inherent in cloud systems, such as data leaks and privacy breaches. This paper provides a comprehensive overview of security techniques in fog computing networks, focusing on the OpenFog reference architecture. Key vulnerabilities, threats and modern approaches to security are discussed, including authentication, encryption, access control and monitoring.

**Keywords:** fog computing; security; OpenFog.

Архитектура туманных вычислений облегчает обработку данных в режиме реального времени, значительно сокращает задержки и повышает общую эффективность и отзывчивость систем IoT. По сравнению с традиционными облачными вычислениями она обрабатывает данные ближе к их источнику.

Несмотря на свои преимущества, fog computing унаследовало уязвимости облачных сред, такие как утечки данных и проблемы конфиденциальности. Кроме того, уникальные характеристики среды Fog, включая ее децентрализованный характер, гетерогенный состав узлов и ограниченность ресурсов этих узлов, создают новые и особые проблемы безопасности [1].

Распределенный характер узлов Fog расширяет потенциальную поверхность атаки, что делает защиту географически распределенных узлов сложной задачей. Близость узлов Fog к конечным пользователям приводит к увеличению сбора конфиденциальных данных.

Разнообразие владельцев и администраторов узлов Fog также усложняет управление доверием. А так как сети туманных вычислений состоят из устройств с разными характеристиками производительности, ресурсами и возможностями безопасности — это затрудняет внедрение единых политик безопасности. [2–3]

Среди предложенных механизмов повышения безопасности туманных вычислений выделим изменение к подходам аутентификации и авторизации, гомоморфное шифрование или шифрование на основе атрибутов и сервисы безопасного хранения (SSS) в среде приложений Cisco IOx.

Также рассмотрим отечественную систему СКАТ [4–6], позволяющую дополнительно усилить безопасность каждого облака. Использование системы должно улучшить централизованный сбор и анализ информации, для разработки сценариев противодействия угроз в будущем [7–9].

Но предложенные методы неэффективны без комплексного подхода с использованием эталонной архитектуры [6], разработанной консорциумом OpenFog и подтвержденной в стандарте IEEE 1934. Архитектура OpenFog основана на восьми ключевых принципах, и безопасность является одним из критически важных аспектов.

В работе предложены основные требования к ее обеспечению в сетях связи на основе туманных вычислений. Ключевыми являются создание аппаратного корня и цепочек доверия [10–11], контроль сбора конфиденциальных данных и непрерывный мониторинг, безопасное управление учетными данными и доменами подключения, а также принятие стандартизированных криптографических функций [12].

Для решения проблем непрерывного мониторинга, создания учетных записей и обязательных доменов с соответствующими предлагается использовать в каждой зоне на границе Fog систему СКАТ, на основе технологии глубокого анализа трафика (DPI). Система также оснащена балансировщиком нагрузки, позволяющим избежать утилизации и потери трафика при обработке, в работе приведено тестирование данного элемента.

По результатам исследования сделаны выводы об эффективности использования СКАТ, особенно в контексте туманных вычислений. В дальнейшем исследование будет направлено на разработку эффективных и облегченных протоколов безопасности при использовании актуальных решений в управлении в сетях туманных вычислений.

## СПИСОК ЛИТЕРАТУРЫ

1. Князьков, В.С. Гибридные вычисления на универсальных и специализированных вычислительных платформах / А. С. Коржавина, В. С. Князьков // Программные Системы: Теория И Приложения. 2020. 29 p.
2. D'Agostino, P. A Scalable Fog Computing Solution for Industrial Predictive Maintenance and Customization / P. D'Agostino, M. Violante, G. Macario // Polytechnic University of Turin. 2024. 14 p.
3. Shiriaev, E. Reliability and Security for Fog Computing Systems / E. Shiriaev, T. Ermakova, E. Bezuglova, M. A. Lapina, M. Babenko // North-Caucasus Federal University. 2024. 15 p.
4. Липатников В.А., Шевченко А.А. Модель процесса управления информационной безопасностью распределенной информационной системы на основе выявления и оценки уязвимостей // Информационные системы и технологии. 2018. № 1(105). С. 114-123.
5. Grossetete, P. Best Security Practices for Fog Computing [Электронный ресурс] URL: <https://blogs.cisco.com/digital/best-security-practices-for-fog-computing> (Дата обращения 29.04.2025)
6. OpenFog Reference Architecture for Fog Computing/ OpenFog Consortium/2017.—162 p.
7. Martin, B.A. OpenFog Security Requirements and Approaches / B. A. Martin, F. Michaud, D. Banks, A. Mosenia, R. Zolfonoon, S. Irwan// IEEE Fog World Congress. 2017. 6 p.



8. Липатников В.А., Шевченко А.А. Проактивное управление информационной безопасностью автоматизированной системы радиоконтроля // Информационные системы и технологии. 2019. № 4(114). С. 112-121.
9. Липатников В.А., Ложечкин А.А., Шевченко А.А. Построение комплексной защиты киберфизической системы от деструктивных воздействий // Информационные системы и технологии. 2020. № 6(122). С. 112-120.
10. Красов, А. В. Метод управления трафиком в гибридной программно-определяемой сети / А. В. Красов, М. В. Левин, А. Ю. Цветков // Информационные технологии и телекоммуникации. 2016. Т. 4, № 2. С. 53-63. EDN XDCOST.
11. Исаченков, П. А. Исследование эффективности метода управления потоками трафика на основе информации о нагрузке в программно-определяемой сети с неравными метриками маршрутов / П. А. Исаченков, А. В. Красов, М. В. Левин // Современная наука и инновации. 2017. № 2(18). С. 32-38. EDN YULDCS.
12. Моделирование защищенной масштабируемой сети предприятия с динамической маршрутизацией на основе IPv6 / Д. В. Сахаров, А. В. Красов, И. А. Ушаков, Э. В. Бирих // Защита информации. Инсайд. 2020. № 1(91). С. 51-57. EDN TONWOS.

УДК 004.056

### ВЛИЯНИЕ ВНЕШНИХ УГРОЗ НА ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Задбоев Вадим Александрович<sup>1</sup>, Кот Ирина Игоревна<sup>2</sup>, Сaitов Никита Михайлович<sup>2</sup>

<sup>1</sup> Военная академия связи им. Маршала Советского Союза С. М. Буденного  
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

<sup>2</sup> Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевикова пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mails: daritergha@gmail.com, sitov.nm@sut.ru, zadboev89@mail.ru

**Аннотация.** Рассматривается анализ влияния внешних угроз на безопасность персональных данных, которые всё чаще используются не только для нарушения доступности, но и как прикрытие для кражи информации. Рассмотрены основные типы атак (L7, L3/L4, volumetric), их механизмы и последствия для критической инфраструктуры. Предложены технические (CDN, WAF, IDS/IPS) и организационные меры защиты (реагирование на инциденты, пентесты, обучение персонала). Разработанная модель системы обеспечивает отказоустойчивость, защиту данных и соответствие требованиям GDPR и ФЗ-152. Подчёркнута важность комплексного подхода к защите персональных данных в условиях растущих киберугроз.

**Ключевые слова:** безопасность; DDoS; атака; Zero Trust; failover.

### IMPACT OF EXTERNAL THREATS ON PERSONAL DATA

Zadboev Vadim<sup>1</sup>, Kot Irina<sup>2</sup>, Saitov Nikita<sup>2</sup>

<sup>1</sup> The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny  
3 Tikhoretsky Av, St. Petersburg, 194064, Russia

<sup>2</sup> The Bonch-Bruевич Saint Petersburg State University of Telecommunications  
22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mails: daritergha@gmail.com, sitov.nm@sut.ru, zadboev89@mail.ru

**Abstract.** The article analyzes the impact of DDoS attacks on the security of personal data, which are increasingly used not only to disrupt availability, but also as a cover for stealing information. The article considers the main types of attacks (L7, L3/L4, volumetric), their mechanisms and consequences for critical infrastructure. Technical (CDN, WAF, IDS/IPS) and organizational protection measures (incident response, pentests, personnel training) are proposed. The developed system model ensures fault tolerance, data protection and compliance with the requirements of the GDPR and Federal Law 152. The importance of an integrated approach to protecting personal data in the face of growing cyber threats is emphasized.

**Keywords:** security, DdoS, attack, Zero Trust, failover.

DDoS-атаки, изначально воспринимавшиеся как угроза доступности сервисов, всё чаще используются как инструмент для маскировки киберпреступлений, включая хищение персональных данных. В условиях цифровизации и роста зависимости организаций от онлайн-инфраструктуры, такие атаки становятся серьёзным риском для информационной безопасности. DDoS-атаки реализуются через ботнеты и делятся на три категории: атаки уровня приложений (L7), протокольные (L3/L4) и объёмные (volumetric), каждая из которых нацелена на перегрузку ресурсов разными способами [1–4].

Хотя основная цель DDoS — вывод сервиса из строя, их последствия могут быть гораздо шире: сбои в работе систем хранения данных, нарушение целостности информации, снижение доверия пользователей, юридические санкции (включая штрафы по GDPR и ФЗ-152) и финансовые потери. Особенно критичны атаки на организации в сфере здравоохранения, финансов и государственных услуг, где недоступность сервисов напрямую влияет на права граждан [5–7].

Для защиты от DDoS и обеспечения сохранности персональных данных требуется комплексный подход. К техническим мерам относятся использование CDN для распределения нагрузки, WAF для фильтрации вредоносных запросов, балансировка нагрузки, системы IDS/IPS для обнаружения аномалий, а также rate limiting и CAPTCHA для противодействия ботам [8–10].



Организационные меры включают разработку и тестирование плана реагирования на инциденты (IRP), регулярные пентесты и нагрузочные испытания, соблюдение нормативных требований по защите данных и обучение персонала основам кибербезопасности [11–12].

В рамках исследования предложена модель защищённой системы, сочетающая отказоустойчивую архитектуру, многоуровневую защиту от DDoS и механизмы обеспечения конфиденциальности и целостности данных даже при частичной компрометации. Решение соответствует стандартам GDPR и Ф3-152, поддерживает масштабируемость и быстрое восстановление после атак [12–14].

Разработанная система демонстрирует эффективность при применении стека технологий, включая облачные платформы, принципы Zero Trust и автоматизированное реагирование. Результаты подчёркивают необходимость комплексной защиты, сочетающей технические, организационные и нормативные аспекты. В перспективе требуется развитие методов прогнозирования атак, внедрение машинного обучения и адаптация к новым, более изощрённым сценариям киберугроз.

#### СПИСОК ЛИТЕРАТУРЫ

1. Ковалёв, Д. С. Современные методы защиты от DDoS-атак / Д. С. Ковалёв, А. В. Логинов // Информационная безопасность. 2020. № 3. С. 45-52. URL: <https://some-journal-link.ru/ddos-methods> (дата обращения: 20.05.2025).
2. Гребнева, М. А. Утечки персональных данных в цифровой экономике: риски и пути минимизации / М. А. Гребнева // Экономическая безопасность. 2022. № 2. С. 112-120.
3. Петров, А. И. Основы кибербезопасности корпоративных сетей / А. И. Петров, Н. В. Смирнов. М.: Технополис, 2019. 278 с.
4. Cloudflare. Understanding DDoS attacks / Cloudflare Resources. URL: <https://www.cloudflare.com/learning/ddos/> (дата обращения: 25.05.2025).
5. Kaspersky Lab. DDoS Protection Solutions. Annual Report 2023 / Kaspersky DDoS Report. URL: <https://www.kaspersky.com/resource-center/attacks-threats/ddos-protection-solutions> (дата обращения: 18.04.2025).
6. Липатников В.А., Шевченко А.А. Модель процесса управления информационной безопасностью распределенной информационной системы на основе выявления и оценки уязвимостей // Информационные системы и технологии. 2018. № 1(105). С. 114-123.
7. ISO/IEC 27001:2013. Information technology Security techniques Information security management systems Requirements. URL: <https://www.iso.org/isoiec-27001-information-security.html> (дата обращения: 22.04.2025).
8. GDPR. General Data Protection Regulation (EU) 2016/679. Official Journal of the European Union. URL: <https://gdpr-info.eu/> (дата обращения: 24.05.2025).
9. Федеральный закон от 27.07.2006 № 152-ФЗ О персональных данных // Российская газета. URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_61801/](http://www.consultant.ru/document/cons_doc_LAW_61801/) (дата обращения: 23.05.2025).
10. Липатников В.А., Шевченко А.А. Проактивное управление информационной безопасностью автоматизированной системы радиоконтроля // Информационные системы и технологии. 2019. № 4(114). С. 112-121.
11. Липатников В.А., Ложечкин А.А., Шевченко А.А. Построение комплексной защиты киберфизической системы от деструктивных воздействий // Информационные системы и технологии. 2020. № 6(122). С. 112-120.
12. Разработка методологии тестирования систем защиты информации в виртуальных комплексах для обнаружения ошибок I и II-рода / А. В. Красов, Р. Р. Максудова, В. В. Нефедов [и др.] // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. № 1. С. 45-52. DOI 10.46418/2079-8199\_2021\_1\_7. EDN AACDXB.
13. Security Decision Support in the Control Systems based on Graph Models / E. V. Doynikova, A. V. Fedorchenko, E. S. Novikova [et al.] // Proceedings of 2021 IV International Conference on Control in Technical Systems (CTS), Saint Petersburg Electrotechnical University "LETI", 21–23 сентября 2021 года. IEEE, 2021. P. 224-227. DOI 10.1109/CTS53513.2021.9562793. EDN SGNONH.
14. Разработка модели обеспечения отказоустойчивости сети передачи данных / Д. В. Сахаров, С. И. Штеренберг, М. В. Левин, Ю. А. Колесникова // Известия высших учебных заведений. Технология легкой промышленности. 2016. Т. 34, № 4. С. 14-20. EDN YNLHLN.

УДК 004.056

#### ИНСТРУМЕНТ ПРОГНОЗИРОВАНИЯ АТАК ВНЕДРЕНИЯ ВРЕДНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

**Задбоев Вадим Александрович, Липатников Валерий Алексеевич, Садовников Владимир Евгеньевич**  
Военная академия связи им. Маршала Советского Союза С. М. Буденного  
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия  
e-mails: zadboev89@mail.ru, vas@mil.ru

**Аннотация.** Представлена модель оценки вероятности атак с использованием байесовских сетей, ориентированная на выявление внедрения вредоносного программного обеспечения в информационно-вычислительных сетях. Подход основан на учёте уязвимостей программного обеспечения, поведенческих факторов пользователей, эффективности средств защиты и индикаторов компрометации. Модель интегрируется с SIEM-системами и позволяет динамически пересчитывать вероятность атаки на основе поступающих данных, что обеспечивает переход от реактивного к прогностическому управлению инцидентами. Приведён пример расчёта апостериорной вероятности, подтверждающий практическую применимость метода. Использование предложенного подхода повышает точность обнаружения угроз и снижает нагрузку на специалистов центров мониторинга безопасности.

**Ключевые слова:** байесовские сети; прогнозирование атак; вредоносное программное обеспечение; информационно-вычислительные сети; анализ киберрисков; SIEM; управление инцидентами.

#### MALWARE ATTACK PREDICTION TOOL

**Zadboev Vadim, Lipatnikov Valeriy, Sadovnikov Vladimir**  
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny  
3 Tikhoretsky Av, St. Petersburg, 194064, Russia  
e-mails: zadboev89@mail.ru, vas@mil.ru

**Abstract.** The article presents a model for assessing the probability of attacks using Bayesian networks, aimed at identifying the introduction of malware into information and computing networks. The approach is based on software vulnerabilities, user behavioral factors, the effectiveness of security tools, and indicators of compromise. The model integrates with SIEM systems and allows dynamically recalculating the probability of an attack based on incoming data, which ensures the transition from reactive to predictive incident management. An example of calculating the a posteriori probability is given, confirming the practical applicability of the method. Using the proposed approach increases the accuracy of threat detection and reduces the workload of security monitoring center specialists.

**Keywords:** Bayesian networks; attack prediction; malware; information technology networks; cyber risk analysis; SIEM; incident management.

Современные информационно-вычислительные сети подвергаются постоянному воздействию кибератак, значительная часть которых связана с внедрением вредоносного программного обеспечения. Традиционные средства защиты — антивирусы, межсетевые экраны, системы предотвращения вторжений — не всегда справляются с полиморфными и целевыми атаками, особенно когда речь идёт о критической инфраструктуре. Это обуславливает необходимость использования методов, которые позволяют не только фиксировать факт инцидента, но и прогнозировать его вероятность на основе совокупности факторов риска [1–2].

Одним из наиболее перспективных подходов является использование байесовских сетей. Данный инструмент позволяет формализовать причинно-следственные связи между различными источниками данных и учитывать неопределённость, что особенно важно в условиях кибербезопасности. В представленной работе предложена модель, ориентированная на прогнозирование атак по внедрению вредоносного ПО. Она учитывает как технические параметры — наличие уязвимостей программного обеспечения, эффективность средств защиты, — так и поведенческие аспекты, связанные с действиями пользователей. Дополнительно анализируются индикаторы компрометации, которые поступают в SIEM-системы в режиме реального времени [3].

Модель реализует принцип динамического пересчёта апостериорной вероятности атаки. Это позволяет переходить от статического анализа угроз к их прогнозированию и раннему выявлению. Пример расчёта показал, что при сочетании высокой степени уязвимости ПО, рискованного поведения пользователей и обнаружении отдельных IoC вероятность атаки возрастает до критического уровня, требующего немедленного реагирования. Такой результат подтверждает практическую значимость предлагаемого подхода [4–5].

Интеграция байесовского модуля в SIEM-системы обеспечивает автоматическое формирование инцидентов при превышении заданных порогов вероятности атаки. Это снижает количество ложных срабатываний и повышает эффективность работы центров мониторинга безопасности. Таким образом, модель не только улучшает точность обнаружения угроз, но и оптимизирует процесс реагирования [6–7].

Вместе с тем, подход имеет ограничения: он чувствителен к корректности исходных данных и требует настройки априорных вероятностей. Однако перспективы развития модели включают интеграцию с методами машинного обучения, использование динамических байесовских сетей для анализа временных зависимостей и подключение внешних источников Threat Intelligence для автоматического обновления базы индикаторов компрометации.

Предложенная модель расчёта вероятности атак позволяет сделать шаг от реактивного к прогностическому управлению инцидентами и является важным элементом стратегии защиты критической информационной инфраструктуры.

## СПИСОК ЛИТЕРАТУРЫ

1. Липатников В.А., Шевченко А.А., Мелехов К.В., Задбоев В.А. Метод активной защиты объектов критической информационной инфраструктуры от кибератак на основе прерывания процесса воздействия нарушителя // Информационно-управляющие системы. 2025. № 2(135). С. 37–49.
2. Патент № 2839562 С1 Российская Федерация, МПК G06F 12/14, H04L 12/22. Способ защиты информационно-вычислительной сети от вторжения : заявл. 27.02.2024 : опубл. 06.05.2025 / В. А. Задбоев, В. А. Липатников, К. В. Мелехов, А. А. Шевченко ; заявитель Федеральное государственное казенное военное образовательное учреждение высшего образования «Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С.М. Буденного» Министерства обороны Российской Федерации. EDN IUBQKF.
3. Использование технологий блокчейн для обеспечения информационной безопасности / В. А. Задбоев, В. Д. Шевяков, М. Д. Беседин, В. Е. Садовников // Современные тенденции развития фундаментальных и прикладных наук : Материалы VIII Всероссийской научно-практической конференции, Брянск, 25 января 2025 года. Брянск: Брянский государственный инженерно-технологический университет, 2025. С. 529–532. EDN VAKRLK.
4. Анализ проблем развития технологий блокчейн для обеспечения информационной безопасности в России / Д. Ю. Изотов, В. А. Задбоев, В. Д. Шевяков, В. Е. Садовников // Современные тенденции развития фундаментальных и прикладных наук : Материалы VIII Всероссийской научно-практической конференции, Брянск, 25 января 2025 года. Брянск: Брянский государственный инженерно-технологический университет, 2025. С. 532–536. EDN GSARHE.
5. Беседин, М. Д. анализ принципов работы DNS-серверов и DDoS-атак / М. Д. Беседин, В. А. Задбоев, В. Р. Полищук // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2024) : Материалы XIII Международной научно-технической и научно-методической конференции, Санкт-Петербург, 27–28 февраля 2024 года. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2024. С. 108–112. EDN LREHBE.
6. Метод повышения защищенности информационно-телекоммуникационной сети с учетом использования средств определения геолокации нарушителя / В. А. Липатников, В. А. Задбоев, К. В. Мелехов, А. А. Шевченко // Труды учебных заведений связи. 2023. Т. 9, № 4. С. 86–96. DOI 10.31854/1813-324X-2023-9-4-86-96. EDN FWQHUC.
7. Антонов, А. С. Анализ областей анализа данных. Цели и стратегии внедрения искусственного интеллекта в аналитику / А. С. Антонов, А. Г. Григоренко, В. А. Задбоев // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2024) : Сборник научных статей XIII Международной научно-технической и научно-методической конференции, Санкт-Петербург, 27–28 февраля 2024 года. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2024. С. 529–531. EDN ANMXZQ.

УДК 004.056

**АНАЛИЗ УЯЗВИМОСТИ MQTT В IOT****Задбоев Вадим Александрович<sup>1</sup>, Шашин Михаил Антонович<sup>2</sup>, Якобсон Дмитрий Алексеевич<sup>2</sup>**<sup>1</sup> Военная академия связи им. Маршала Советского Союза С. М. Буденного  
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия<sup>2</sup> Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mails: zadboev89@mail.ru, vas@mil.ru

**Аннотация.** В статье на практическом примере описан полный цикл пентеста — от сетевой разведки с помощью Nmap до эксплуатации уязвимостей в конфигурации MQTT-брокеров, используемых в IoT-системах. Особое внимание уделено перехвату и анализу служебных сообщений, а также выполнению команд через MQTT-интерфейс. Результаты исследования подчёркивают важность правильной настройки брокера, использования надёжной аутентификации и регулярного обновления ПО для обеспечения безопасности IoT-инфраструктуры.

**Ключевые слова:** MQTT; IoT-безопасность; MQTT Брокер; пентест; защита данных.

**MQTT VULNERABILITY ANALYSIS IN IOT****Zadboev Vadim<sup>1</sup>, Shashin Mikhail<sup>2</sup>, Jakobson Dmitriy<sup>2</sup>**<sup>1</sup> The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny (Military Academy of Telecommunications)

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

<sup>2</sup> The Bonch-Bruевич Saint Petersburg State University of Telecommunications

22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia

e-mails: zadboev89@mail.ru, vas@mil.ru

**Abstract.** The article describes a full pentest cycle using a practical example — from network reconnaissance using Nmap to exploiting vulnerabilities in the configuration of MQTT brokers used in IoT systems. Particular attention is paid to intercepting and analyzing service messages, as well as executing commands via the MQTT interface. The results of the study emphasize the importance of properly configuring the broker, using reliable authentication, and regularly updating the software to ensure the security of the IoT infrastructure.

**Keywords:** MQTT; It Security; MQTT Broker; pentest; data protection.

Протокол MQTT, изначально разработанный как легковесное решение для передачи данных по принципу «публикация/подписка», сегодня широко используется в IoT-инфраструктурах благодаря своей эффективности в условиях ограниченной пропускной способности, что делает его ключевым элементом в системах с граничными вычислениями и распределёнными сетями. Несмотря на популярность, MQTT-брокеры зачастую становятся объектами кибератак из-за слабой защиты и типовых ошибок в конфигурации, что подчёркивает необходимость проведения регулярных тестов на проникновение [1–3].

Первый этап пентеста — сетевая разведка — осуществляется с помощью Nmap с параметрами определения версий сервисов, запуска скриптов и детального вывода, что позволяет выявить открытые порты и потенциально уязвимые MQTT-сервисы.

Подписка на все топики MQTT-брокера (с использованием # в качестве wildcard) позволяет злоумышленнику перехватывать широкий спектр данных, включая информацию о подключённых устройствах, их статусах и конфигурациях, особенно при отсутствии аутентификации и шифрования [4–5].

Анализ трафика выявил передачу конфигурационных данных в кодировке Base64, декодирование которых раскрыло критически важную информацию, включая список поддерживаемых команд, среди которых — возможность выполнения произвольных системных команд (например, через CMD). Сложная и маскирующая структура топиков может использоваться для сокрытия функционала, однако при детальном анализе такие механизмы легко обходятся, что делает их недостаточной мерой защиты [6–7].

Практические эксперименты подтвердили возможность выполнения команд через MQTT-интерфейс при доступе к защищённым топикам, что указывает на серьёзные уязвимости в архитектуре и настройке брокеров. Основные риски связаны с отсутствием изоляции конфигурационных топиков, слабой или отсутствующей аутентификацией, а также передачей управляющих команд без дополнительной верификации на уровне полезной нагрузки [8–10].

Для обеспечения безопасности IoT-систем на основе MQTT необходимо внедрять многоуровневую защиту: строгую аутентификацию, шифрование трафика (TLS), ограничение доступа к топикам, регулярное обновление ПО и изоляцию критических интерфейсов. Регулярное тестирование на проникновение и мониторинг MQTT-трафика должны стать обязательными компонентами процесса эксплуатации IoT-инфраструктур для своевременного выявления и устранения уязвимостей.

**СПИСОК ЛИТЕРАТУРЫ**

1. Миняев, А. А. Моделирование угроз безопасности информации в территориально-распределённых информационных системах / А. А. Миняев // Научные технологии в космических исследованиях Земли. 2021. Т. 13, № 2. С. 52–65. DOI 10.36724/2409-5419-2021-13-2-52-65. EDN OJBTHU.
2. Миняев, А. А. Метод и методика оценки эффективности системы защиты территориально-распределённых информационных систем / А. А. Миняев // Информатизация и связь. 2020. № 6. С. 29–36. EDN ESJFSC.

3. Миняев, А. А. Методика оценки эффективности системы защиты информации территориально-распределенных информационных систем / А. А. Миняев, А. В. Красов // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 3. С. 26-32. DOI 10.46418/2079-8199\_2020\_3\_4. EDN YNHOEI.
4. Зосимова Марина Александровна, Смирнов Сергей Александрович ИОТ. К вопросу об интернете вещей // Вестник Пермского университета. Серия: Математика. Механика. Информатика. 2023.
5. Баев Д. А., Волков Р. О., Зонов А. Д. Мониторинг безопасности в ИОТ-сетях // StudNet. 2021.
6. Каженова Ж. С., Кенжебаева Ж. Е. Безопасность в протоколах и технологиях ИОТ: обзор // International Journal of Open Information Technologies. 2022. № 3. URL: <https://cyberleninka.ru/article/n/bezopasnost-v-protokolah-i-tehnologiyah-iot-obzor> (дата обращения: 04.06.2025).
7. Исаева Ольга Сергеевна, Кулясов Никита Владимирович, Исаев Сергей Владиславович Инфраструктура сбора данных и имитации угроз безопасности сети интернета вещей // Сибирский аэрокосмический журнал. 2025. №1. URL: <https://cyberleninka.ru/article/n/infrastruktura-sbora-dannyh-i-imitatsii-ugroz-bezopasnosti-seti-interneta-veschey> (дата обращения: 04.06.2025).
8. Липатников В. А., Шевченко А.А. Методика проактивного управления информационной безопасностью распределенной информационной системы на основе интеллектуальных технологий // Информационные системы и технологии. 2022. № 2(130). С. 107-115.
9. Липатников В. А., Шевченко А.А. Математическая модель процесса управления информационной безопасностью распределенной информационной системы в условиях несанкционированного воздействия злоумышленника // Информационные системы и технологии. 2022. № 3(131). С. 121-130.
10. Липатников В.А., Шевченко А.А., Мелехов К.В., Задбоев В.А. Метод активной защиты объектов критической информационной инфраструктуры от кибератак на основе прерывания процесса воздействия нарушителя // Информационно-управляющие системы. 2025. № 2(135). С. 37-49.

УДК 004.056.53

## ВИРТУАЛИЗАЦИЯ МЕЖСЕТЕВЫХ ЭКРАНОВ КАК ИНСТРУМЕНТ ПОВЫШЕНИЯ ОТКАЗОУСТОЙЧИВОСТИ И БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ СЕТЕЙ

Зуев Дмитрий Павлович

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mail: dmitriy.molodec88@gmail.com

**Аннотация.** Рассматриваются особенности применения виртуализированных межсетевых экранов в корпоративных сетях. Показано, что переход от аппаратных решений к программно-ориентированным (Virtual NGFW) позволяет повысить гибкость инфраструктуры, ускорить развёртывание сервисов и реализовать отказоустойчивые кластеры без значительных аппаратных затрат. На примере программного продукта UserGate VE500 показаны ключевые свойства: поддержка гипервизоров VMware, Hyper-V и KVM; интеграция с корпоративными сервисами аутентификации; использование технологий глубокого анализа трафика (DPI), предотвращения вторжений (IPS) и SSL-инспекции. В докладе акцентируется внимание на практических аспектах: применимости решения для учебных стендов, удобстве управления и соответствия нормативным требованиям.

**Ключевые слова:** виртуализация; виртуальный межсетевой экран; отказоустойчивость; безопасность сети; UserGate VE500.

## VIRTUALIZATION OF FIREWALLS AS A TOOL FOR INCREASING FAULT TOLERANCE AND SECURITY OF CORPORATE NETWORKS

Zuev Dmitry

The Bonch-Bruevich Saint Petersburg State University of Telecommunications  
22 Bolshhevikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mail: dmitriy.molodec88@gmail.com

**Abstract.** Discusses the features of applying virtualized firewalls in corporate networks. The transition from hardware solutions to software-based Virtual NGFW is shown to increase infrastructure flexibility, accelerate service deployment, and implement high-availability clusters without significant hardware investments. Using UserGate VE500 as an example, key properties are highlighted: support for VMware, Hyper-V, and KVM hypervisors; integration with corporate authentication services; utilization of Deep Packet Inspection (DPI), Intrusion Prevention System (IPS), and SSL inspection. The focus is placed on practical aspects such as applicability in training environments, management convenience, and compliance with regulatory requirements.

**Keywords:** virtualization; virtual firewall; UserGate VE500; high-availability cluster; network security; DPI; IPS.

Рост интенсивности киберугроз и усложнение векторов атак предопределяют необходимость внедрения комплексных средств защиты периметра, способных противостоять не только известным угрозам, но и новым, ранее не документированным сценариям злоумышленников. Современные кибератаки, как правило, носят многоэтапный, мультивекторный и распределённый характер, что существенно затрудняет их идентификацию традиционными средствами мониторинга. Помимо этого, всё чаще фиксируются атаки с применением элементов искусственного интеллекта и машинного обучения, что требует от защитных систем способности к постоянному обучению и адаптации. Появляются примеры использования генеративных моделей для обхода сигнатурных систем защиты, а также атак, на основе автоматизированных ботнетов, которые способны адаптироваться к условиям среды и изменять свою тактику в реальном времени. Дополнительно фиксируется рост числа атак на цепочки поставок (supply chain attacks), кибершпионаж с применением целевых фишинговых кампаний и

эксплойтов нулевого дня, что делает актуальной необходимость многоуровневого подхода к защите [1]. В этих условиях аппаратные решения, хотя и обеспечивают высокий уровень надёжности, демонстрируют фундаментальные ограничения: они основаны на статически заданной архитектуре, имеют низкую эластичность при масштабировании и не способны в полной мере адаптироваться к изменяющимся условиям корпоративной инфраструктуры [2]. Для крупных корпораций это оборачивается значительными капитальными затратами и длительными циклами внедрения, тогда как для малых и средних предприятий — снижением адаптивности к трансформации бизнес-процессов и ограниченными возможностями по соответствию регуляторным нормам. Кроме того, при возникновении необходимости интеграции новых бизнес-направлений или подключения внешних партнёров аппаратные решения часто требуют существенной модернизации, сопряжённой с затратами времени на сертификацию и тестирование.

На фоне массового перехода организаций к облачным сервисам, гибридным ИТ-моделям и виртуализированным средам особую актуальность приобретает парадигма использования виртуализированных межсетевых экранов нового поколения (NGFW). Эти программно-ориентированные решения позволяют динамически адаптировать архитектуру защиты в соответствии с меняющимися условиями, минимизируя финансовые и временные издержки и формируя оптимальный баланс между уровнем безопасности и экономической рациональностью [3]. Они обладают встроенными возможностями интеграции с экосистемами автоматизации, а также могут быть включены в процессы DevSecOps для обеспечения защиты на всех стадиях жизненного цикла приложений. Дополнительно такие решения поддерживают автоматическое обновление политик безопасности в зависимости от контекста, что особенно важно при работе с распределёнными командами и удалёнными пользователями [4]. Подобные системы особенно востребованы у организаций, функционирующих в условиях ограниченных ресурсов, но обязанных соблюдать строгие регуляторные требования в области информационной безопасности, включая международные стандарты ISO/IEC, национальные законы о персональных данных и отраслевые регламенты. Внедрение виртуализированных NGFW способствует как повышению уровня соответствия нормативным предписаниям, так и снижению совокупной стоимости владения ИТ-инфраструктурой, а также обеспечивает возможности для унификации процессов аудита, управления инцидентами и интеграции с платформами управления рисками. Важным преимуществом является и возможность демонстрации уровня защищённости перед инвесторами и страховыми компаниями, что способствует снижению страховых премий и повышению доверия к бизнесу.

Функциональные возможности NGFW выходят далеко за рамки классической фильтрации пакетов, включая механизмы глубокого анализа трафика (DPI), обнаружение и предотвращение вторжений (IPS), инспекцию зашифрованного трафика (SSL), контроль приложений и учетных записей пользователей, предотвращение утечек данных, а также интеграцию с SIEM-платформами для централизованного мониторинга и аналитики. Ключевое преимущество заключается в способности оперативной адаптации под конкретные бизнес-контексты и задачи. Например, в случае проведения слияний и поглощений или при интеграции дочерних компаний в единую инфраструктуру организации возможность быстрого развертывания виртуальных узлов приобретает критическое значение. Так, при необходимости масштабирования корпоративной сети или сегментации трафика можно в кратчайшие сроки развернуть дополнительные виртуальные узлы, не прибегая к приобретению специализированного оборудования. Это не только снижает капитальные расходы и ускоряет внедрение новых сервисов, но и обеспечивает гибкость в условиях высокой динамики организационных структур и интенсивного внедрения инноваций. Для компаний, ориентированных на инновационное развитие, данная эластичность приобретает стратегическое значение, позволяя вводить новые цифровые продукты и сервисы без компромиссов в области безопасности. Более того, возможность интеграции с инструментами оркестрации и контейнеризации, расширяет сферу применения NGFW, делая их частью современной архитектуры облачных приложений и поддерживающей концепции микросервисов и CI/CD [5].

Кластеризация виртуализированных межсетевых экранов обеспечивает высокую отказоустойчивость и гарантирует непрерывность ключевых бизнес-процессов. При отказе одного из узлов система автоматически выполняет переключение на резервный компонент, минимизируя временные простои и снижая вероятность утраты критически важной информации [6]. Такой механизм соответствует базовым принципам информационной безопасности, включая доступность сервисов, целостность и конфиденциальность данных. Дополнительно кластерная архитектура упрощает апробацию новых политик безопасности, тестирование сценариев реагирования на инциденты и моделирование гипотетических атак в контролируемой среде. Это делает виртуальные кластеры не только инструментом промышленной эксплуатации, но и исследовательской платформой для анализа киберугроз и выработки методологических подходов к их нейтрализации [3]. Более того, данные возможности могут служить основой для формирования специализированных центров компетенций по кибербезопасности в корпоративных и академических средах. В рамках образовательного процесса такие кластеры используются для симуляции сценариев атак и разработки новых алгоритмов обнаружения, что способствует подготовке высококвалифицированных специалистов, а также способствует развитию сотрудничества между университетами и индустрией. В перспективе такие платформы могут интегрироваться с национальными инициативами по киберсуверенитету и формированию глобальных альянсов в области киберобороны.

Таким образом, организации, внедряющие виртуализированные NGFW, получают не просто механизм фильтрации трафика, но и интегративную платформу, эволюционирующую синхронно с ИТ-ландшафтом предприятия, централизованно управляемую и масштабируемую. Подобный подход формирует фундамент для

построения адаптивной, устойчивой и экономически обоснованной системы киберзащиты, соответствующей современным вызовам, перспективным требованиям и готовой к интеграции с облачными платформами [7].

#### СПИСОК ЛИТЕРАТУРЫ

1. Колосков Н.В., Прохоров А.С. Практика развёртывания систем информационной безопасности в виртуальной среде // Журнал прикладной информатики. 2024. №2. С. 45-53.
2. Тетеркин В. Ф., Митрошин А. А., Чернышев С. В. Регламент сопровождения межсетевого экрана, сертифицированного ФСТЭК // Материалы Междунаро. научно-практ. конф. по обеспечению комплексной безопасности предприятий: проблемы и решения. 2015. С. 95.
3. Ерышов В. Г., Клименко А. А. Типы, классы, обзор современных межсетевых экранов, сертифицированных по требованиям ФСТЭК // Обработка, передача и защита информации в компьютерных системах. 2022. С. 205-207.
4. Штеренберг, С. И. Архитектура защищенной интеллектуальной системы обнаружения вторжений и инцидентов в распределенных информационных системах / С. И. Штеренберг // Региональная информатика и информационная безопасность Сборник трудов Санкт-Петербургской международной конференции, Санкт-Петербург, 25–27 октября 2023 года. СПб: СПОИСУ, 2023. С. 321-326.
5. Оценка статистических характеристик различных типов фреймов IEEE 802.11 для сервисов местоположения / В. А. Петров, М. М. Ковцур, А. Ю. Киструга, С. И. Штеренберг // Информационная безопасность регионов России (ИБРР-2021) : Материалы XII Санкт-Петербургской межрегиональной конференции, Санкт-Петербург, 27–29 ноября 2021 года. СПб: СПОИСУ, 2021. С. 187-188.
6. Штеренберг, С. И. разработка сценариев безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения / С. И. Штеренберг, А. И. Москальчук, А. В. Красов // Информационные технологии и телекоммуникации. 2021. Т. 9, № 1. С. 47-58.
7. Штеренберг, С. И. Анализ свойств децентрализованных рассинхронизированных пакетных нейросетевых программ в распределенной информационной системе / С. И. Штеренберг, А. В. Поляничева, Е. Н. Талакин // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2024. № 3. С. 45-51.

УДК 004.056

#### БЕЗОПАСНОСТЬ НЕЙРОННЫХ СЕТЕЙ В СИСТЕМАХ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ ТРАНСПОРТНЫХ СРЕДСТВ

**Киркум Глеб Константинович, Сиргазинов Тимур Муратович, Шевченко Александр Александрович**  
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mails: kirkum.gk@sut.ru, sirgazinov.tm@sut.ru, alex\_pavel1991@mail.ru

**Аннотация.** В условиях активного внедрения технологий искусственного интеллекта в городскую инфраструктуру особую актуальность приобретает вопрос обеспечения информационной безопасности систем умных парковок. Основой таких систем является нейросетевой модуль распознавания государственных регистрационных знаков, который обрабатывает видеопоток и принимает решения о доступе. Однако данный компонент подвержен различным видам атак, включая подмену видеоданных, внедрение адверсариал-примеров, отравление обучающих выборок, кражу модели и манипуляции через API. В работе проведён анализ уязвимостей и предложен комплекс мер по защите, включающий антиспуфинг, шифрование, изоляцию среды исполнения, контроль доступа и поведенческий мониторинг. Реализация этих подходов позволяет повысить устойчивость системы к киберугрозам и сохранить достоверность процессов идентификации.

**Ключевые слова:** безопасность нейросетей; умная парковка; атаки на входы; защита данных; антиспуфинг; контроль доступа.

#### ENSURING INFORMATION SECURITY OF SMART PARKING SYSTEMS

**Kirkum Gleb, Sirgazinov Timur, Shevchenko Aleksandr**  
The Bonch-Bruevich Saint Petersburg State University of Telecommunications  
22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mails: kirkum.gk@sut.ru, sirgazinov.tm@sut.ru, alex\_pavel1991@mail.ru

**Abstract.** As artificial intelligence technologies are increasingly integrated into urban infrastructure, ensuring the information security of smart parking systems has become critically important. The core of such systems is a neural network module for recognizing vehicle license plates, which processes video streams and makes access decisions. However, this component is susceptible to various attacks, including video feed spoofing, adversarial example injection, training data poisoning, model theft, and API manipulation. This paper presents an analysis of vulnerabilities and proposes a comprehensive set of protection measures, including anti-spoofing, encryption, execution environment isolation, access control, and behavioral monitoring. Implementing these strategies enhances the system's resilience against cyber threats and ensures the reliability of identification processes.

**Keywords:** neural network security; smart parking; adversarial attacks; data protection; anti-spoofing; access control.

Современные системы умных парковок всё чаще полагаются на нейросетевые технологии для автоматизированного распознавания государственных регистрационных знаков транспортных средств. Такие системы, являясь частью интеллектуальных решений в городской инфраструктуре, обеспечивают бесконтактный контроль доступа, учёт времени пребывания и автоматическое взаимодействие с платёжными сервисами. Однако широкое использование видеопотока, персональных данных автомобилей и программных моделей искусственного интеллекта делает их потенциально уязвимыми к целому спектру киберугроз [1–3].

Нейросетевой модуль, отвечающий за обработку изображений и принятие решений по идентификации, становится ключевой точкой риска. Анализ возможных атак показывает, что злоумышленники могут

осуществлять физическую подмену видеопотока, внедрять адверсариял-примеры через визуальные помехи на номерах, проводить отравление обучающих выборок при наличии механизмов дообучения, а также пытаться скомпрометировать модель путём её экстракции или несанкционированного доступа через API [4–6].

Дополнительную опасность представляет возможность подделки ответов системы и внесение ложных записей в базу данных проездов. Эти угрозы требуют комплексного подхода к обеспечению информационной безопасности [7–9]. Предлагается ряд мер, направленных на повышение устойчивости нейросетевого модуля. К ним относятся шифрование модели и её хранение в защищённом формате, применение контейнеризации для изоляции вычислительной среды, использование антиспуфинговых механизмов, основанных на анализе динамических характеристик видео — таких как микродвижения камеры, блики света, тени и временные задержки реакции.

Важным элементом защиты является строгий контроль доступа к API с использованием JWT-токенов, двухфакторной аутентификации, ограничения частоты запросов и фильтрации по доверенным IP-адресам. Особое внимание уделяется детекции аномалий: все случаи сбоев распознавания, массовые обращения к системе или необычные паттерны поведения должны фиксироваться в журнале событий и анализироваться службой безопасности [10–12].

Внедрение таких мер позволяет не только защитить конфиденциальность и целостность данных, но и обеспечить отказоустойчивость системы в условиях многоэтапных атак. Предложенный подход способствует созданию защищённой и надёжной инфраструктуры умных парковок, сохраняя высокую степень автоматизации и минимизируя риск компрометации.

#### СПИСОК ЛИТЕРАТУРЫ

1. Лапина М. А., Ржевская Н. В., Котляров Д. В., Дюдюк Г. Д. Особенности организации атак на нейронные сети для распознавания образов // Электронный научный журнал Курского государственного университета «Auditorium». 2023. № 2 (38) [Электронный ресурс]. URL: [https://api-mag.kursksu.ru/api/v1/get\\_pdf/4948/](https://api-mag.kursksu.ru/api/v1/get_pdf/4948/) (дата обращения: 04.05.2025).
2. Мачикина Е. П. Анализ схемы электронной подписи видеопотока // журнал Сибирского государственного университета телекоммуникаций и информатики «Вестник СибГУТИ». Том 17. 2023. № 1. С. 46–51.
3. Намиот Д. Е. Введение в атаки отравлением на модели машинного обучения // International Journal of Open Information Technologies. Т. 11. 2023. № 3. С. 58–68.
4. Ерболатов А. Н. Реверс-инжиниринг против искусственного интеллекта: анализ самозащищенных моделей ИИ // Международный научный журнал «Вестник науки». Том 4. 2025. №2. С. 436–443.
5. Липатников В.А., Шевченко А.А. Модель процесса управления информационной безопасностью распределенной информационной системы на основе выявления и оценки уязвимостей // Информационные системы и технологии. 2018. № 1(105). С. 114–123.
6. Липатников В.А., Шевченко А.А. Проактивное управление информационной безопасностью автоматизированной системы радиоконтроля // Информационные системы и технологии. 2019. № 4(114). С. 112–121.
7. Арзамасцев Н. А. Особенности использования искусственных нейронных сетей в сфере информационной безопасности // Научный журнал «StudNet». Том 5. 2022. №5. С. 3936–3945.
8. Липатников В.А., Ложечкин А.А., Шевченко А.А. Построение комплексной защиты киберфизической системы от деструктивных воздействий // Информационные системы и технологии. 2020. № 6(122). С. 112–120.
9. Research and Evaluation of the Most Significant Quantitative Characteristics of MPLS Equipment / A. Krasov, P. Karelsky, I. Zuyev [et al.] // Smart Innovation, Systems and Technologies. 2021. Vol. 220. P. 431–443. DOI 10.1007/978-981-33-6632-9\_38. EDN KHZCLM.
10. Использование математических методов прогнозирования для оценки нагрузки на вычислительную мощность IoT-сети / Д. В. Сахаров, А. М. Гельфанд, А. А. Казанцев, И. Е. Пестов // Научно-аналитический журнал Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. 2020. № 2. С. 86–94. EDN DLMENI.
11. Миняев, А. А. Моделирование угроз безопасности информации в территориально-распределенных информационных системах / А. А. Миняев // Наукоемкие технологии в космических исследованиях Земли. 2021. Т. 13, № 2. С. 52–65. DOI 10.36724/2409-5419-2021-13-2-52-65. EDN OJBGTU.
12. Задача интеллектуальной защиты информационно-телекоммуникационной сети на основе анализа враждебных действий и цепочек вторжений / В. А. Задбоев, В. А. Липатников, К. В. Мелехов, В. А. Робак // Региональная информатика и информационная безопасность : Сборник трудов Санкт-Петербургской международной конференции и Санкт-Петербургской межрегиональной конференции, Санкт-Петербург, 23–25 октября 2024 года. Санкт-Петербург: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2024. С. 93–97. EDN APXUGP.

УДК 004.056

#### ДЕКОМПОЗИЦИЯ ТРЕБОВАНИЙ ОЦЕНКИ ЗАЩИЩЕННОСТИ ОБЪЕКТА КИИ ПО ФУНКЦИОНАЛЬНОМУ НАЗНАЧЕНИЮ

Киселёв Николай Николаевич

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Большевицкое пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

e-mail: mr.nikkis@mail.ru

**Аннотация.** Доклад посвящен методологии декомпозиции требований к защите объектов критической информационной инфраструктуры для целей оценки их защищенности. Основной акцент сделан на необходимости разделения требований на документарные, которые универсальны для субъекта КИИ и регламентируют систему управления безопасностью и объектно-ориентированные, которые специфичны для конкретного объекта, его функционального назначения, конфигурации и условий эксплуатации. Предлагается подход к группировке декомпозированных требований по функциональным направлениям защиты с учетом обязательного базового комплекса документов объекта КИИ определяемого приказом ФСТЭК России № 239. В основу анализа положена практика автора по оценке соответствия объектов КИИ.

**Ключевые слова:** критическая информационная инфраструктура; оценка защищенности; декомпозиция требований; документарные требования; объектно-ориентированные требования; функциональная группировка требований; аттестация объектов КИИ.

## DECOMPOSITION OF SECURITY ASSESSMENT REQUIREMENTS FOR CII FACILITIES BY FUNCTIONAL PURPOSE

Kiselev Nikolay

The Bonch-Bruевич Saint Petersburg State University of Telecommunications

22 Bolshhevikov Av, bldg 1, St. Petersburg, 193232, Russia

e-mail: mr.nikkis@mail.ru

**Abstract.** The article is devoted to the methodology of decomposition of requirements for the protection of critical information infrastructure objects for the purpose of assessing their security. The main emphasis is placed on the need to separate requirements into documentary requirements, which are universal for the subject of critical information infrastructure and regulate the security management system, and object-oriented requirements, which are specific to a particular object, its functional purpose, configuration and operating conditions. An approach is proposed to grouping decomposed requirements by functional areas of protection, taking into account the mandatory basic set of documents of the critical information infrastructure object determined by the order of the FSTEC of Russia No. 239. The analysis is based on the author's practice of assessing the conformity of critical information infrastructure objects.

**Keywords:** critical information infrastructure; security assessment; decomposition of requirements; documentary requirements; object-oriented requirements; functional grouping of requirements, certification of critical information infrastructure objects.

Эффективная оценка защищенности объекта критической информационной инфраструктуры требует детального анализа выполнения требований действующего законодательства [1], распространяющихся как на наличие и содержание обязательной документации, так и на фактическую реализацию и настройку технических средств защиты. Одной из ключевых проблем является адаптация общих норм к специфике конкретного объекта. В данной статье рассматриваются требования предъявляемые к объекту КИИ зафиксированные в Приказе 239 ФСТЭК России [2]. Одно из возможных решений видится в декомпозиции требований с последующей группировкой по функциональному назначению. Такой подход учитывает принципиальное различие между документарным уровнем и уровнем конкретной практической реализации на объекте КИИ. Рассматриваемый подход является своего рода развитием идеи декларативного схем и подхода к управлению информационной безопасностью объекта, о котором в своих работах упоминают такие отечественные ученые, как Ерохин С.Д., Петухов А.Н., Пилюгин П.Л., которые занимались вопросам обеспечения безопасности критических информационных инфраструктур [3].

Идея излагаемого решения возникла в процессе деятельности по аттестации объектов КИИ в процессе их эксплуатации и аттестации [4]. В настоящем материале данная идея получила развитие и представлена в доработанном виде. Основная идея заключается в том, что декомпозированные требования целесообразно сгруппировать по их функциональному назначению.

В предлагаемом подходе декомпозиция рассматривается как одна из основ оценки состояния защищенности объекта КИИ. Процесс разбиения общих норм Приказа 239 ФСТЭК России на атомарные, проверяемые утверждения, применимые к объекту с возможностью указания бинарной оценки о выполнении предлагается проводить и разбивать на группы следующим образом. Необходимо до начала процедуры оценки определить какая их часть относится к документарному обеспечению. То есть что должно быть прописано в регламентах, политиках, актах. И какая часть требует конкретной реализации и проверки конфигурации на самом объекте или оборудовании. То есть что именно должно быть настроено и работать.

При этом следует отметить роль обязательной документации в декомпозиции. Для каждого объекта или группы объектов должен быть разработан базовый документный комплекс, который является исходной точкой для проверки документарных требований. Каждый документ декомпозируется на проверяемые параметры согласно логике предлагаемого подхода.

В качестве примера рассмотрим несколько укрупненную декомпозицию документарных требований, которую можно применить для Акта категорирования, являющегося обязательным и одним из основных документов объекта критической информационной инфраструктуры:

- формальные требования — соответствие форме, наличие подписи, даты, номера;
- сведения об объекте — корректность наименования, адреса, сферы деятельности, назначения, архитектуры;
- сведения о субъекте — корректность наименования, адреса, данных о руководителе и ответственном подразделении;
- сетевые взаимодействия — корректность данных о сетях связи, операторах, целях и способах взаимодействия;
- эксплуатация — корректность данных об эксплуатирующей организации, ее реквизитах, элементах объекта;
- технические средства — корректность описания оборудования, ПО (общесистемного, прикладного), средств защиты информации;



- сведения об УБИ — корректность указания актуальных категорий нарушителей, УБИ (идентификаторы, наименования), типов инцидентов;
- категория значимости — корректность присвоенной категории, показателей критериев;
- меры защиты — актуальность указанного состава организационных и технических мер.

Ключевым шагом на данном этапе является анализ каждого требования декомпозированного требования [5–8], так как это будет оказывать влияние на оценку защищенности. На данном этапе анализ документов через формальные недостатки документации, даже при удовлетворительном состоянии технических мер, позволит понять как организованы работы по обеспечению безопасности объекта КИИ. Очевидно, что при суммировании оценок это снижают общую оценку защищенности, так как свидетельствуют о неэффективности системы управления безопасностью и повышает риски реализации угроз.

На следующем этапе, здесь стоит сделать оговорку на то, что в реальных условиях данные этапы могут переплетаться или идти параллельно друг другу проверяются объектно-ориентированные (прикладные) требования, которые направлены на непосредственную реализацию мер защиты на конкретном объекте КИИ.

Их основная особенность заключается в том, что они специфичны и достаточно жестко определяются следующими параметрами:

- функциональное назначение объекта;
- конкретной технологической платформой (операционная система, база данных, оборудование);
- актуальной конфигурацией (настройки безопасности могут меняться с выявлением новых угроз);
- условиями эксплуатации (сетевое окружение, физическое расположение);
- обрабатываемыми категориями информации;
- результатами категорирования и моделью угроз безопасности информации.

В качестве примера можно привести параметры, которые должны быть отражены в эксплуатационной документации:

- конкретные настройки межсетевых экранов;
- параметры парольной политики на серверах;
- конфигурация правил разграничения доступа к базам данных;
- настройки журналирования;
- параметры обновления ПО;
- физическая защита конкретного серверного помещения.

Декомпозиция требований оценки защищенности объекта КИИ, основанная на четком разделении документарного и объектно-ориентированного аспектов, с последующей компоновкой по функциональным направлениям защиты, является методологическим подходом, который позволяет:

1. Системно адаптировать общие требования ФСТЭК 239 к уникальным характеристикам объекта.
2. Четко разграничить зоны ответственности за обеспечение требований между подразделениями ответственными за организацию системы управления безопасностью и подразделениями, осуществляющими эксплуатацию объекта.
3. Построить структурированную и проверяемую модель оценки защищенности объекта КИИ, основанную на функциональном назначении требований.
4. Эффективно использовать обязательный пакет документов объекта КИИ как основу для проверки документарных требований, а также в качестве опоры для проверок осуществляемых непосредственно на объекте критической информационной инфраструктуры.

Одним из значимых условий эффективности оценки является актуальность и качество документарной базы. Комплексный подход, учитывающий как наличие и правильность документации, так и корректность технической реализации мер защиты, обеспечивает достоверную оценку реального уровня защищенности объекта КИИ.

## СПИСОК ЛИТЕРАТУРЫ

1. ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ (последняя редакция) // Собрание законодательства РФ. 2017. № 31 (часть I). Ст. 4736. [Электронный ресурс]. URL: base.garant.ru (дата обращения: 05.08.2025)
2. Приказ Федеральной службы по техническому и экспортному контролю «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры РФ» от 25.12.2017 №239 // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: publication.pravo.gov.ru (дата обращения: 05.08.2025).
3. Ерохин, С. Д. Управление безопасностью критических информационных инфраструктур / С. Д. Ерохин, А. Н. Петухов, П. Л. Пилюгин. Москва Научно-техническое издательство «Горячая линия-Телеком», 2021. 240 с. ISBN 978-5-9912-0916-8. EDN AKWARB.
4. Киселев, Н. Н. Метод автоматизации процедуры аттестации объектов критической информационной инфраструктуры в удаленных регионах России / Н. Н. Киселев // Вопросы защиты информации. 2025. № 1(148). С. 53-58. DOI 10.52190/2073-2600\_2025\_1\_53. EDN JVLLXU.
5. Миняев, А. А. Методика оценки эффективности системы защиты информации территориально-распределенных информационных систем / А. А. Миняев, А. В. Красов // Вестник СПбГУПТД: Естественные и технические науки. 2020. № 3. С. 26-32. DOI 10.46418/2079-8199\_2020\_3\_4. EDN YNHQEI.
6. Типовые офтальмологические информационные системы, являющиеся объектами критической информационной инфраструктуры / А. В. Красов, Н. Н. Лансере, И. И. Фадеев [и др.] // Офтальмохирургия. 2022. № S4. С. 85-91. DOI 10.25276/0235-4160-2022-4S-85-91. EDN CBKURN.
7. Актуальные угрозы безопасности информации в сфере здравоохранения и офтальмологии / А. В. Красов, Д. Н. Шакин, Н. Н. Лансере [и др.] // Офтальмохирургия. 2022. № S4. С. 92-101. DOI 10.25276/0235-4160-2022-4S-92-101. EDN IYQQXV. (КИИ категорирование).
8. Майоров, А. В. Модель представления Больших данных о компьютерных атаках в формате posql / А. В. Майоров, А. В. Красов, И. А. Ушаков // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2023. № 2. С. 47-54. DOI 10.46418/2079-8199\_2023\_2\_9. EDN GDZKWM.

УДК 004.056.53

## ПРАКТИКА ПОСТРОЕНИЯ УСТОЙЧИВОЙ К АТАКАМ ИНФРАСТРУКТУРЫ НА ОСНОВЕ ПРОТОКОЛА LORAWAN

**Красников Даниил Андреевич, Ковцур Максим Михайлович, Никифоров Александр Вячеславович**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Большевикова пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

e-mails: dkrasnikov7604@mail.ru, maxkovzur@mail.ru, obsx@ya.ru

**Аннотация.** В тезисах представлен обзор современных методов и практик усиления защиты данных в сетях LoRaWAN, критически важных для развертывания безопасного Интернета вещей (IoT). На основе анализа встроенных криптографических механизмов протокола и их ключевых уязвимостей (таких как риски компрометации ключей в ABP, атаки на процедуру OTAA и уязвимость к RF-глушению) предложен и обоснован комплекс дополнительных мер безопасности. Делается вывод о необходимости применения многоуровневой защиты, сочетающей аппаратные Security-модули, мониторинг сетевого трафика и организационные меры, для противодействия современным киберугрозам.

**Ключевые слова:** LoRaWAN; IoT; кибербезопасность; шифрование; аутентификация; RF-глушение; аппаратные модули безопасности.

## PRACTICE OF BUILDING ATTACK-RESISTANT INFRASTRUCTURE BASED ON THE LORAWAN PROTOCOL

**Krasnikov Daniil, Kovzur Maxim, Nikiforov Alexander**

The Bonch-Bruевич Saint Petersburg State University of Telecommunications

22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia

e-mails: dkrasnikov7604@mail.ru, maxkovzur@mail.ru, obsx@ya.ru

**Abstract.** The abstract presents a review of modern methods and practices for enhancing data protection in LoRaWAN networks, which are critical for the deployment of a secure Internet of Things (IoT). Based on an analysis of the protocol's built-in cryptographic mechanisms and their key vulnerabilities (such as the risks of key compromise in ABP, attacks on the OTAA procedure, and vulnerability to RF jamming), a set of additional security measures is proposed and justified. It is concluded that it is necessary to apply multi-level protection, combining hardware Security-modules, network traffic monitoring and organizational measures, to counteract modern cyber threats.

**Keywords:** LoRaWAN; IoT; cybersecurity; encryption; authentication; RF-jamming; hardware security modules.

Широкое распространение энергоэффективных IoT-решений на базе LoRaWAN делает их привлекательной мишенью для злоумышленников. LoRa (Long Range) — технология модуляции для маломощной беспроводной связи. Она обеспечивает передачу данных на большие расстояния с низким энергопотреблением. [1] Несмотря на встроенные механизмы защиты, стандартный протокол обладает рядом уязвимостей, что требует разработки и внедрения современных методов обеспечения безопасности на всех уровнях сети.

Цель работы — анализ ограничений стандартных средств безопасности LoRaWAN и систематизация дополнительных методов построения защищенной IoT-инфраструктуры.

Основные результаты:

1. Классифицированы ключевые угрозы. Помимо replay-атак и DoS, наибольшую опасность представляют уязвимости методов активации (ABP и OTAA), а также отсутствие защиты от RF-глушения.

2. Оценены стандартные механизмы. Такие средства, как сквозное AES-шифрование, MIC и счетчики сообщений, обеспечивают базовый, но не достаточный уровень безопасности.

3. Предложен комплекс мер защиты. Для повышения устойчивости необходима многоуровневая стратегия, включающая: Аппаратный уровень — Security-чипы (напр., ATECC608A) для защиты ключей, Сетевой уровень — Мониторинг трафика (IPS) [2] для выявления аномалий, Организационный уровень — VPN, обновления ПО [3] и строгий контроль доступа.

Надежная защита сетей LoRaWAN требует комплексного подхода, выходящего за рамки стандартных средств. Ключевое значение имеет интеграция аппаратных модулей безопасности и систем проактивного мониторинга.

## СПИСОК ЛИТЕРАТУРЫ

1. Карманов А.А., Савостин А.А. Технология LoRa как средство цифровой радиотелеметрии для IoT устройств // Вестник СКУ им. М. Козыбаева. 2023. №1 (57). С. 100-106.
2. Петрова Т.В., Ковцур М.М., Карельский П.В., Поляничева А.В. Подходы обнаружения беспроводной точки доступа злоумышленника в локальной вычислительной сети // Региональная информатика (РИ-2022). СПб.: СПОИСУ, 2022. С. 572-573.
3. Цифровая трансформация и проблемы информационной безопасности : Монография / И. А. Альбовский, И. Л. Андреевский, М. Д. Васильев, С. И. Штеренберг [и др.] ; Под ред. А.В. Солодяникова, И.Н. Васильевой. Санкт-Петербург : СПбГЭУ, 2023. 118 с. ISBN 978-5-7310-6193-3. EDN QRTWNK.

УДК 004.051

**ГОМОМОРФНОЕ ШИФРОВАНИЕ КАК ЗАЩИТА КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ****Куклина Маргарита Игоревна, Романова Александра Михайловна,  
Шевченко Александр Александрович**

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: alex\_pavel1991@mail.ru, kuklina\_mi@gmail.com, romanova\_am@gmail.com

**Аннотация.** Развитие шестого поколения сетей связи сопровождается ростом угроз информационной безопасности и увеличением объема персональных данных, обрабатываемых в облачных и распределённых системах. В этих условиях особое значение приобретает использование гомоморфного шифрования, позволяющего выполнять вычисления с зашифрованными данными без раскрытия исходной информации. Рассмотрены ключевые направления применения данной технологии в 6G-средах, включая облачные вычисления, системы машинного обучения и биометрическую аутентификацию. Обосновывается актуальность внедрения полностью гомоморфных схем для повышения уровня доверия к цифровым сервисам и минимизации рисков утечек.

**Ключевые слова:** защита данных; гомоморфное шифрование; 6G; облачные вычисления; безопасность.

**HOMOMORPHOUS ENCRYPTION AS A DATA PRIVACY PROTECTION****Kuklina Margarita, Romanova Alexandra, Shevchenko Aleksandr**

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: alex\_pavel1991@mail.ru, kuklina\_mi@gmail.com, romanova\_am@gmail.com

**Abstract.** The evolution of sixth-generation communication networks is accompanied by increasing cybersecurity threats and the growing volume of personal data processed in cloud and distributed environments. In this context, homomorphic encryption plays a crucial role, enabling computations on encrypted information without disclosing the original data. This paper highlights the main directions of its application in 6G networks, including cloud computing, machine learning systems, and biometric authentication. The adoption of fully homomorphic schemes is emphasized as a key factor in strengthening trust in digital services and reducing data leakage risks.

**Keywords:** data protection; homomorphic encryption; 6G; cloud computing; security.

Современные тенденции в области связи характеризуются стремительным переходом к 6G, что сопровождается ростом числа цифровых сервисов и увеличением объема передаваемой информации. Одновременно возрастает количество угроз, связанных с утечкой и неправомерным использованием данных, что делает задачу защиты конфиденциальности одной из наиболее актуальных.

Гомоморфное шифрование становится важным инструментом в условиях 6G, так как позволяет выполнять вычисления с зашифрованными данными, не требуя их раскрытия. Такой подход снижает вероятность утечек на стороне серверов и обеспечивает новый уровень защиты персональной информации. Особенно значимым это становится для облачных вычислений, где обрабатываются большие массивы медицинских, финансовых и биометрических данных [1–3].

Применение гомоморфного шифрования в задачах машинного обучения открывает возможность построения моделей без раскрытия исходных выборок. Это обеспечивает сохранность персональных данных и делает возможным использование интеллектуальных алгоритмов в сферах с повышенными требованиями к безопасности. Примеры практических решений включают работу с кредитным скорингом и биометрическими системами идентификации, где конфиденциальность имеет ключевое значение [4–6].

Дополнительное внимание уделяется вопросам аутентификации в 6G-сетях. Наряду с традиционными паролями активно развиваются биометрические методы, что требует интеграции криптографических технологий для повышения уровня надежности. Важным направлением выступает также совершенствование DLP-систем, которые в сочетании с гомоморфным шифрованием и методами семантического анализа способны существенно повысить эффективность защиты информации [7–10].

Несмотря на перспективность технологии, остаются нерешенными задачи, связанные с вычислительными затратами и сложностью интеграции полностью гомоморфных схем в существующую инфраструктуру. В дальнейшем предполагается разработка более оптимизированных алгоритмов, способных сочетать высокий уровень безопасности с практической применимостью в масштабных 6G-сетях [11, 12].

Таким образом, гомоморфное шифрование в сочетании с новыми подходами к аутентификации и предотвращению утечек данных формирует основу для построения безопасных цифровых экосистем. Эта технология может стать ключевым элементом обеспечения доверия в эпоху 6G, где защита информации является критически важным фактором развития общества и экономики.

**СПИСОК ЛИТЕРАТУРЫ**

1. Вопросы применения прикладной гомоморфной криптографии // Вопросы кибербезопасности URL: <https://cyberleninka.ru/article/n/voprosy-primeneniya-prikladnoy-gomomorfnoy-kriptografii> (дата обращения: 01.07.2025).
2. Гомоморфизм в криптографии // Молодой исследователь Дона. URL: <https://cyberleninka.ru/article/n/gomomorfizm-v-kriptografii> (дата обращения: 02.07.2025).

3. Гомоморфное шифрование в базах данных // Интеллектуальные технологии на транспорте URL: <https://cyberleninka.ru/article/n/gomomorfnoe-shifrovanie-v-bazah-dannyh> (дата обращения: 01.07.2025).
4. Гомоморфное шифрование // Труды Института системного программирования РАН URL: <https://cyberleninka.ru/article/n/gomomorfnoe-shifrovanie> (дата обращения: 03.07.2025).
5. Методы полностью гомоморфного шифрования на основе матричных полиномов // Вопросы кибербезопасности URL: <https://cyberleninka.ru/article/n/metody-polnostyu-gomomorfno-go-shifrovaniya-na-osnove-matrichnyh-polinomov> (дата обращения: 01.07.2025).
6. Ограниченно гомоморфные схемы шифрования // Наука, образование и культура URL: <https://cyberleninka.ru/article/n/ogranichenno-gomomorfnye-shemy-shifrovaniya> (дата обращения: 04.07.2025).
7. Особенности классификации и фильтрации трафика сети передачи данных 6G // Труды МАИ URL: <https://cyberleninka.ru/article/n/osobennosti-klassifikatsii-i-filtratsii-trafika-seti-peredachi-dannyh-6g> (дата обращения: 04.07.2025).
8. Липатников В.А., Шевченко А.А. Проактивное управление информационной безопасностью автоматизированной системы радиоконтроля // Информационные системы и технологии. 2019. № 4(114). С. 112-121.
9. Липатников В.А., Ложечкин А.А., Шевченко А.А. Построение комплексной защиты киберфизической системы от деструктивных воздействий // Информационные системы и технологии. 2020. № 6(122). С. 112-120.
10. Липатников В.А., Шевченко А.А. Модель процесса управления информационной безопасностью распределенной информационной системы на основе выявления и оценки уязвимостей // Информационные системы и технологии. 2018. № 1(105). С. 114-123.
11. Модель управления потоками трафика в программно-определяемой сети с изменяющейся нагрузкой / А. В. Красов, М. В. Левин, С. И. Штеренберг, П. А. Исаченков // Наукоемкие технологии в космических исследованиях Земли. 2016. Т. 8, № 4. С. 70-74. EDN WNEHJT.
12. Миняев, А. А. Метод и методика оценки эффективности системы защиты территориально-распределенных информационных систем / А. А. Миняев // Информатизация и связь. 2020. № 6. С. 29-36. EDN ESJFSC.

УДК 004.056

## СИСТЕМЫ ПОДДЕРЖКИ КРИТИЧЕСКОЙ ОЦЕНКИ ИНФОРМАЦИИ КАК СРЕДСТВО БОРЬБЫ С КОМПЬЮТЕРНЫМИ АТАКАМИ ТИПА ФИШИНГ

Лагутина Светлана Викторовна<sup>1</sup>, Виткова Лидия Андреевна<sup>2</sup>

<sup>1</sup> Санкт-Петербургский государственный университет телекоммуникаций им. Проф. М.А. Бонч-Бруевича  
Большевики пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

<sup>2</sup> СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия

e-mails: LSVBonch@yandex.ru, vitkova@comsec.spb.ru

**Аннотация.** В статье рассмотрены манипулятивные тактики, используемые злоумышленниками при проведении фишинговых кампаний, и предпосылки для создания систем поддержки критической оценки информации с использованием больших языковых моделей для обеспечения автоматизированной подсветки потенциально манипулятивных участков текста и их интерпретируемости (подсказки) в зависимости от уровня подготовки пользователя, в том числе в режиме обучения пользователей.

**Ключевые слова:** фишинг; фишинговые техники; фишинговые письма; анти-фишинговые методы; манипулятивные тактики фишинга; критическое мышление; критическая оценка информации.

## INFORMATION CRITICAL ASSESSMENT SUPPORT SYSTEMS AS AN ANTI-PHISHING METHOD

Lagutina Svetlana<sup>1</sup>, Vitkova Lidia<sup>2</sup>

<sup>1</sup> The Bonch-Bruevich Saint Petersburg State University of Telecommunications  
22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia

<sup>2</sup> St. Petersburg Federal Research Center of the Russian Academy of Sciences  
39 14th Line VO, St. Petersburg, 199178, Russia

e-mails: LSVBonch@yandex.ru, vitkova@comsec.spb.ru

**Abstract.** The article considers manipulative tactics used by attackers in phishing campaigns and the prerequisites for creating systems to support critical information evaluation using large language models to provide automated highlighting of potentially manipulative text sections and their interpretability (hints) depending on the level of user training, including in the user training mode.

**Keywords:** phishing; phishing emails; phishing technique; anti-phishing method; manipulative tactics; critical thinking; information critical assessment.

В настоящее время вместе с бурным развитием технологического стека цифровых продуктов развиваются технологии их защиты, обеспечивающие проактивный поиск угроз, в том числе в обфускационном коде, близкую к реальному времени блокировку нелегитимных соединений, включая отключение скомпрометированных ресурсов, предиктивную аналитику, создание активнов-приманок и «песочниц» для перенаправления усилий злоумышленников и изучения поведения ассоциированных с ними сущностей и вредоносного программного обеспечения, совершенствуются методы защиты, реализующие концепцию «нулевого доверия» (Zero Trust) при разграничении доступа и назначении полномочий, двухфакторную аутентификацию, шифрование, периодическую проверку защищенности, в том числе с помощью автоматизированных средств (Security Validation) и прочее. Для проникновения в такую защищенную информационную систему и сокрытия следов своего присутствия злоумышленник должен обладать большим объемом знаний.

Поэтому в настоящее время АРТ (Advanced Persistent Threat) группировки стали привлекать злоумышленников с навыками психологов и социальных инженеров. Согласно свежему исследованию Positive Technologies «Актуальные

киберугрозы: IV квартал 2024 года — I квартал 2025 года», опубликованному 20.03.2025 [1], атаки с использованием методов социальной инженерии на организации составляют 50% от общего числа атак, а на частных лиц - 88%. Основным каналом социальной инженерии для организаций остается электронная почта (84%), для частных лиц — сайты (44%). Вместе с тем в атаках на частных лиц увеличилась доля использования социальных сетей и мессенджеров.

Все приемы социальной инженерии эксплуатируют психологические особенности человека и влияют на процесс принятия им решений. Злоумышленники используют технологические достижения, такие как искусственный интеллект (ИИ), для повышения точности и масштабируемости кампаний социальной инженерии. Инструменты разведки на основе ИИ помогают злоумышленникам адаптировать свои сообщения к поведению жертв, делая их более убедительными. Для предотвращения атак с применением методов социальной инженерии, как правило, используют технические меры защиты, такие как многофакторная аутентификация, технологии фильтрации электронной почты и системы обнаружения угроз [2], в том числе с применением технологий искусственного интеллекта, и меры, направленные на обучение пользователей по вопросам информационной безопасности.

При этом в статье [3], описывающей исследования различных типов атак с использованием социальной инженерии, такие как претекстинг, целевой фишинг, смишинг, килинг, «водопой», «услуга за услугу», вишинг, фарминг и другие приводится информация о том, что основной причиной 95% кибератак с применением методов социальной инженерии, является недостаточная осведомленность сотрудников о кибербезопасности и небрежность при проверке легитимности URL-адресов. Поэтому для повышения эффективности в борьбе с такими атаками проводят периодическое обучение сотрудников организации (Security Awareness) — тренинги, семинары, курсы по информационной безопасности. Но меры повышения осведомленности сотрудников носят, как правил, периодический характер и проводятся один раз в 3–6 месяцев. При этом, если у сотрудника не выработан навык критического отношения к получаемой информации, он становится легкой жертвой для злоумышленника, особенно в тех случаях, когда сотрудник находится в состоянии функционального нарушения когнитивных функций — стресс, усталость, плохое самочувствие, состояние перегрузки («цейтнота»).

Таким образом, возникает необходимость в системах, которые бы обеспечивали автоматизированную подсветку потенциально манипулятивных участков текста и их объяснение (подсказки) в зависимости от уровня подготовки пользователя, в том числе в режиме обучения пользователей.

Приведем несколько примеров манипулятивных тактики фишинга в корпоративных письмах. Создание ощущения срочности: злоумышленник оставляет получателю ограниченное время на то, чтобы отреагировать на сообщение, что заставляет жертву действовать поспешно и необдуманно. Запугивание и угрозы, игра на страхе: злоумышленники угрожают жертве санкциями против организации или нее самой, чтобы заставить её потерять самообладание и совершить целевое действие, например, открытие файла или переход по ссылке. Игра на любопытстве или рутинных событиях: отправка счетов, уведомлений об оплате или иных документов от имени подрядчиков или заказчиков. Это лишь небольшая часть манипулятивных тактик, используемых злоумышленниками [4].

При этом часть манипулятивных тактик распознаются человеком сложнее, чем другие. В исследовании [5] разделили фишинговые электронные письма на несколько категорий и провели исследование с участием 55 пользователей, чтобы оценить точность выявления фишинга в этих категориях. Исследователи пришли к выводу, что участники более точно распознают фишинговые письма, в которых делается попытка оказать давление, намекая на то, что другие получатели действовали аналогичным образом. В то же время сложнее распознать фишинговые письма, которые играют на эмоциях и имитируют общение со знакомыми людьми с использованием разговорного стиля.

Проверка наличия таких конструкций и выдача подсказок о том, что целесообразно проверить до выполнения каких-либо действий, например, проверить правильность написания почты отправителя, наличие данных о размещении информации на корпоративном порте в случае получения писем от внутренних служб, наличие контактных телефоном, адресов электронной почты и прочее, поможет пользователю отнестись критически к письму. Для выделения таких конструкций могут быть использованы большие языковые модели.

Выделение манипулятивных тактик, свойственных фишинговым письмам, стратегий распознавания фишинга для пользователей разного уровня осведомленности в вопросах информационной безопасности и применение больших языковых моделей для их автоматического выявления в тексте является предметом будущих исследований автора.

## СПИСОК ЛИТЕРАТУРЫ

1. Актуальные киберугрозы: IV квартал 2024 года — I квартал 2025 года // Positive Technologies URL: <https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iv-kvartal-2024-goda-i-kvartal-2025-goda/#id2> (дата обращения: 25.08.2025).
2. Акейбер Х. Дж. Эволюция атак с использованием социальной инженерии: взгляд инженера по кибербезопасности // *AI-Rafidain Journal of Engineering Sciences*. 2025. С. 294–316.
3. Биртрия С. К., Ахлат П., Джайн А. К. Всесторонний анализ атак с использованием социальной инженерии: таксономия атак, стратегии предотвращения и смягчения последствий // *Журнал прикладных исследований в области безопасности*. 2025. Т. 20. № 2. С. 244–292.
4. Проблемы безопасности информационной сферы в условиях информационного противоборства / Л. А. Виткова, А. А. Проноза, Д. В. Сахаров, А. А. Чечулин // *Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018)* : VII Межд. научно-техн. и научно-методич. конф.. Сб. науч. статей. В 4-х т., Санкт-Петербург, 28 февраля 01 2018 года / Под ред. С.В. Бачевского. Т. 1. СПб.: СПбГУ телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2018. С. 191–195. EDN UTRRUC.
5. Чампа А. И. и др. «Сладость или гадость»: исследование того, как люди распознают манипулятивные тактики в фишинговых письмах // *Международная конференция по компьютерной безопасности, надёжности и защите*. Cham : Springer Nature Switzerland, 2025. С. 299–311.

УДК 004.056.55

**МЕТОДИКА ОЦЕНКИ СТОЙКОСТИ МЕТОДА ФОРМИРОВАНИЯ БИТ СЫРОГО КЛЮЧА  
В ПРОТОКОЛЕ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ НА ОСНОВЕ ОЦЕНКИ РАЗНОСТИ  
ПЕРЕДАВАЕМЫХ ОТСЧЁТОВ ПРИ ПРИМЕНЕНИИ АТАКИ  
НА ОСНОВЕ ПОСТРОЕНИЯ РЕШАЮЩЕЙ ТАБЛИЦЫ**

**Лапшин Алексей Сергеевич**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mail: scodec.la@gmail.com

**Аннотация.** Представлена методика оценки стойкости протокола распределения ключей, не использующего криптографические предположения. Методика основана на численном моделировании статистической атаки с построением решающей таблицы. Показано, что практическая стойкость протокола обеспечивается вычислительной сложностью наиболее эффективного варианта атаки.

**Ключевые слова:** распределение ключей; постквантовая криптография; формирование сырого ключа; анализ стойкости; статистическая атака; безопасность физического уровня.

**METHODOLOGY FOR ROBUSTNESS ASSESSMENT OF THE RAW KEY GENERATION METHOD  
IN A KEY DISTRIBUTION PROTOCOL BASED ON THE DIFFERENCE OF TRANSMITTED  
SAMPLES USING A LOOKUP TABLE-BASED ATTACK**

**Lapshin Alexey**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications  
22 Bolshhevikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mail: scodec.la@gmail.com

**Abstract.** A methodology for evaluating the security of a two-stage key distribution protocol that does not use cryptographic assumptions is presented. The methodology is based on the numerical simulation of a statistical attack involving the construction of a lookup table. It is shown that the practical security of the protocol is ensured by the computational complexity of the most effective attack variant.

**Keywords:** key distribution; post-quantum cryptography; raw key generation; security analysis; statistical attack; physical layer security.

Проблема распределения секретных ключей между пользователями является одной из ключевых в современных инфокоммуникационных системах. Большинство классических протоколов [1] опираются на вычислительную сложность математических задач, что делает их потенциально уязвимыми для атак с использованием квантовых компьютеров [2]. В связи с этим актуальной задачей является разработка и анализ протоколов, стойкость которых основана на иных принципах.

В данных тезисах представлена методика оценки практической стойкости двухэтапного протокола распределения ключей, не использующего криптографические предположения. Рассматриваемый протокол включает этап формирования сырого ключа (ФСК) на основе разности отсчётов и этап преимущественного улучшения основного канала (ПУОК) [3]. Предлагаемая методика заключается в детальном анализе и численном моделировании наиболее эффективной стратегии атаки на данный протокол — атаки на основе построения решающей таблицы.

Целью нарушителя в данной методике является установление статистической корреляции между всей совокупностью общедоступных данных, перехваченных в ходе работы протоколов ФСК и ПУОК, и итоговым значением ключа пользователя А. В качестве вектора наблюдаемых данных нарушитель использует перехваченные зашумленные числа, их квантованное значение разности, а также вектор  $\gamma$ , передаваемый на этапе ПУОК. Построив такую таблицу на этапе предварительной оффлайн-симуляции, нарушитель может использовать ее для более точного предсказания секретного бита в реальном времени.

Для оценки эффективности атаки было проведено численное моделирование для трех ее вариантов, отличающихся объемом используемой информации. Результаты показали, что данный алгоритм позволяет нарушителю снизить вероятность ошибки по сравнению с базовой мажоритарной стратегией.

Проведенный анализ показывает, что практическая стойкость протокола, таким образом, обеспечивается не теоретической невозможностью взлома, а экспоненциальным ростом требуемых вычислительных ресурсов при увеличении ключевого параметра протокола  $S$ . Это позволяет гибко настраивать компромисс между производительностью системы и требуемым уровнем ее безопасности.

**СПИСОК ЛИТЕРАТУРЫ**

1. Коржик В. И., Яковлев В. А. Основы криптографии: учебное пособие. Санкт-Петербург: НЦ Интермедиа, 2016. 296 с.
2. Shor P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // SIAM Journal on Scientific and Statistical Computing. 1997. Т. 26, № 5. С. 1484–1509.
3. Yakovlev V., Korzhik V., Akhmetshina M., Zhuvikin A. Key Sharing Protocol Using Exchange by Integers over Public Noiseless Channels Between Users that Provides Security without Cryptographic Assumptions // The International Conference on Information and Telecommunication Technologies. 2020.

УДК 004.056

**МОДЕЛИРОВАНИЕ СЕТЕВОГО ПОВЕДЕНИЯ КЛИЕНТСКИХ ОС  
ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ IDS****Легкодымов Даниил Михайлович, Староверов Андрей Игоревич,  
Шевченко Александр Александрович, Щёголев Ефим Константинович**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

e-mails: alex\_pavel1991@mail.ru, danillegk65@gmail.com, staroverov\_ai@gmail.com, efimshchogolev@gmail.com

**Аннотация.** Рассматривается метод обнаружения сетевых атак, основанный на моделировании характерных профилей сетевого поведения клиентских операционных систем. В отличие от традиционных систем обнаружения вторжений, рассматриваемый подход учитывает специфику реализации сетевых стеков и фоновой активности различных ОС, что позволяет формировать более точные признаки для классификации потоков. Проведённые эксперименты на датасете CIC-IDS2017 показали, что использование индивидуальных профилей устройств в сочетании с алгоритмами машинного обучения (Random Forest, XGBoost, CatBoost) обеспечивает точность классификации атак свыше 0,99 при минимальной доле ложных срабатываний. Полученные результаты демонстрируют, что учёт операционной среды конечного устройства является значимым фактором для повышения адаптивности и надёжности систем сетевой безопасности.

**Ключевые слова:** профили сетевой активности; операционные системы; интеллектуальные методы; обнаружение вторжений; адаптивные IDS.

**MODELING CLIENT OS NETWORK BEHAVIOR TO IMPROVE IDS EFFICIENCY****Legkodymov Daniil, Staroverov Andrey, Shevchenko Alexander, Shchogolev Yefim**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

22 Bolshevnikov Av, bldg 1, St. Petersburg, 193232, Russia

e-mails: alex\_pavel1991@mail.ru, danillegk65@gmail.com, staroverov\_ai@gmail.com, efimshchogolev@gmail.com

**Abstract.** The article considers a method for detecting network attacks based on modeling characteristic profiles of network behavior of client operating systems. Unlike traditional intrusion detection systems, the approach under consideration takes into account the specifics of the implementation of network stacks and background activity of various OS, which allows for the formation of more accurate features for flow classification. Experiments conducted on the CIC-IDS2017 dataset showed that the use of individual device profiles in combination with machine learning algorithms (Random Forest, XGBoost, CatBoost) provides an accuracy of attack classification over 0.99 with a minimum proportion of false positives. The results obtained demonstrate that taking into account the operating environment of the end device is a significant factor in increasing the adaptability and reliability of network security systems.

**Keywords:** network activity profiles; operating systems; intelligent methods; intrusion detection; adaptive IDS.

Развитие методов обнаружения атак в сетевом трафике напрямую связано с необходимостью повышения надёжности и адаптивности систем информационной безопасности. Традиционные системы обнаружения вторжений (IDS) в большинстве случаев опираются на обобщённые модели анализа трафика, что снижает их точность и приводит к увеличению количества ложных тревог.

В современных условиях целесообразным представляется использование профилирования, основанного на особенностях клиентских операционных систем, поскольку именно они определяют характер сетевого взаимодействия конечных устройств [1–3].

В настоящем исследовании предложен подход, заключающийся в построении индивидуальных профилей сетевого поведения для различных ОС, что позволяет учитывать различия в реализации протоколов TCP/IP, особенности фоновой активности и характер приложений. Такой учёт специфики даёт возможность выделять признаки, наиболее значимые для классификации атак. В качестве исходных данных использован открытый набор CIC-IDS2017, содержащий реальные дампы сетевого трафика с разметкой. Из него были сформированы поднаборы по типам клиентских ОС, что обеспечило возможность сравнения результатов при одинаковых условиях эксперимента [4–6].

После предобработки данных и балансировки классов были выделены признаки, отражающие статистические параметры потоков и особенности взаимодействия протоколов.

Для решения задачи классификации применялись алгоритмы Random Forest, XGBoost и CatBoost, которые обучались и тестировались на сбалансированных выборках. Метрики качества продемонстрировали высокую точность детектирования атак: для всех моделей показатели accuracy не опускались ниже 0,973, а лучшие результаты достигали уровня 0,995–0,996.

Наиболее устойчивыми оказались модели градиентного бустинга, особенно CatBoost, который на ряде поднаборов превзошёл другие алгоритмы по всем ключевым метрикам [7–8].

Полученные результаты показывают, что профилирование трафика с учётом ОС не только позволяет повысить точность обнаружения атак, но и существенно снижает число ложных срабатываний, что особенно важно для промышленных IDS.

В отличие от обобщённых подходов, где признаки формируются без учёта операционной среды, предложенная методика использует профильные данные и тем самым обеспечивает более релевантное обучение моделей. Такой подход делает систему более адаптивной к изменению условий функционирования и открывает перспективы её применения в реальном времени [9–11].

Сравнение с результатами других исследований подтверждает, что полученные метрики сопоставимы или превосходят показатели новейших моделей, включая ансамблевые и глубокие нейронные сети. При этом специфика предлагаемого метода заключается в ориентации на индивидуализацию поведения конечных устройств. Это может быть особенно полезно для анализа атак, нацеленных на конкретные платформы, где обобщённые модели часто оказываются менее эффективными [12–13].

В то же время метод имеет ряд ограничений. Использование одного датасета и ограниченного числа типов атак снижает универсальность модели, а высокая зависимость от качества исходных данных требует дополнительных проверок на других платформах.

Перспективным направлением дальнейших исследований является включение более разнообразных наборов данных, расширение числа исследуемых операционных систем, включая мобильные и IoT-устройства, а также применение гибридных архитектур с использованием глубокого обучения. Эти шаги позволят создать новое поколение IDS, сочетающих высокую точность детектирования, устойчивость к новым угрозам и способность к динамической адаптации в условиях изменяющейся сетевой среды.

#### СПИСОК ЛИТЕРАТУРЫ

1. Disha R. A., Waheed S. Performance analysis of machine learning models for intrusion detection system using Gini Impurity-based Weighted Random Forest (GIWRF) feature selection technique // *Cybersecurity*. 2022. Vol. 5, № 1.
2. Saleem M., Azam M., Mubeen Z., Mumtaz G. Machine learning for improved threat detection: LightGBM vs. CATBoost // *Journal of Computing & Biomedical Informatics*. 2024. Vol. 7, № 1. P. 571-580.
3. Yurkin, D. V. Formation of the instantaneous information security audit concept / D. V. Yurkin, I. I. Livshitz, A. A. Minyaev // *Communications in Computer and Information Science*. 2016. Vol. 678. P. 314-324. DOI 10.1007/978-3-319-51917-3\_28. EDN YVGPXZ.
4. Al-Obaidi A., Ibrahim A. A., Khaleel A. M. The effectiveness of deploying machine learning techniques in information security to detect nine attacks: UNSW-NB15 dataset as a case study // *Mathematical Modelling of Engineering Problems*. 2023. Vol. 10, № 5. P. 1557-1565.
5. Майоров, А. В. Модель представления Больших данных о компьютерных атаках в формате nosql / А. В. Майоров, А. В. Красов, И. А. Ушаков // *Вестник СПбГУПТД. Серия 1: Естественные и технические науки*. 2023. № 2. С. 47-54. DOI 10.46418/2079-8199\_2023\_2\_9. EDN GDZKWM.
6. Легкодымов Д. М., Левшун Д. С. Подход к профилированию устройств Интернета вещей для обнаружения вредоносной активности // *Региональная информатика (РИ-2024): материалы XIX Санкт-Петербургской международной конференции, Санкт-Петербург, 23–25 октября 2024 г.* Санкт-Петербург: СПб ОИВТССУ, 2024. С. 119-121.
7. Kurniabudi K., Stiawan D., Darmawijoyo D. et al. Important features of CICIDS-2017 dataset for anomaly detection in high dimension and imbalanced class dataset // *Indonesian Journal of Electrical Engineering and Informatics (IJEI)*. 2021. Vol. 9, № 2. P. 498-511.
8. Canadian Institute for Cybersecurity. CICIDS2017 dataset [Электронный ресурс]. URL: <https://www.unb.ca/cic/datasets/ids-2017.html> (дата обращения: 01.06.2025).
9. Исследование рынка жилья Российской Федерации с использованием методов добычи знаний / Ю. А. Леонов, Л. Б. Филиппова, А. А. Мартыненко, И. И. Живодовский // *Известия Тульского государственного университета. Технические науки*. 2024. № 2. С. 87-93.
10. Липатников В. А., Шевченко А.А. Методика проактивного управления информационной безопасностью распределенной информационной системы на основе интеллектуальных технологий // *Информационные системы и технологии*. 2022. № 2(130). С. 107-115.
11. Липатников В. А., Шевченко А.А. Математическая модель процесса управления информационной безопасностью распределенной информационной системы в условиях несанкционированного воздействия злоумышленника // *Информационные системы и технологии*. 2022. № 3(131). С. 121-130.
12. Липатников В.А., Шевченко А.А., Мелехов К.В., Задбоев В.А. Метод активной защиты объектов критической информационной инфраструктуры от кибератак на основе прерывания процесса воздействия нарушителя // *Информационно-управляющие системы*. 2025. № 2(135). С. 37-49.
13. Использование математических методов прогнозирования для оценки нагрузки на вычислительную мощность IoT-сети / Д. В. Сахаров, А. М. Гельфанд, А. А. Казанцев, И. Е. Пестов // *Научно-аналитический журнал Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России*. 2020. № 2. С. 86-94. EDN DLMENr.

УДК 004.056

#### ОЦЕНКА БЕЗОПАСНОСТИ МОДЕЛИ РАЗГРАНИЧЕНИЯ ДОСТУПА В KUBERNETES: ОТ АУДИТА КОНФИГУРАЦИЙ К ПОИСКУ ВЕКТОРОВ АТАК

Мастеница Евгений Александрович

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mail: eugene.mastenitsa@yandex.ru

**Аннотация.** В работе рассматриваются практические сложности анализа безопасности ролевых моделей доступа (RBAC) в среде Kubernetes. Показано, что традиционные подходы к тестированию на проникновение и аудиту конфигураций часто недостаточны для выявления уязвимостей, связанных с избыточными привилегиями и некорректным распределением ролей. Предлагается методика систематической оценки RBAC-конфигураций, ориентированная на выявление скрытых векторов атак и потенциальных путей повышения привилегий. Особое внимание уделяется использованию специализированных инструментов и анализу журналов аудита для повышения точности оценки и обеспечения более полного понимания реального распределения прав внутри кластера.

**Ключевые слова:** Kubernetes; ролевое управление доступом; информационная безопасность; управление привилегиями; модели угроз; оценка уязвимостей.



## SECURITY ASSESSMENT OF THE ACCESS RESTRICTION MODEL IN KUBERNETES: FROM CONFIGURATION AUDIT TO ATTACK VECTOR SEARCH

Mastenitsa Evgeniy

The Bonch-Bruевич Saint Petersburg State University of Telecommunications  
22 Bolshhevikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mail: eugene.mastenitsa@mail.ru

**Abstract.** This paper examines the practical challenges of analyzing the security of role-based access control (RBAC) models in Kubernetes. It demonstrates that traditional penetration testing and configuration audit methods are often insufficient to detect vulnerabilities related to over-permissioning and improper role assignments. A systematic methodology for assessing RBAC configurations is proposed, focusing on the identification of hidden attack vectors and potential privilege escalation paths. Particular attention is given to the use of specialized tools and audit log analysis to improve the accuracy of assessment and to provide a more comprehensive understanding of actual permission distribution within the cluster.

**Keywords:** Kubernetes; Role-Based Access Control; information security; privilege management; threat modeling; vulnerability assessment.

Обеспечение безопасности в контейнерных средах Kubernetes является комплексной задачей, где модель ролевого управления доступом (RBAC) играет центральную роль. Однако на практике именно конфигурации RBAC часто становятся источником скрытых уязвимостей [1].

Стандартные процедуры тестирования на проникновение, как правило, сосредоточены на анализе уязвимостей в образах контейнеров или сетевых политиках, в то время как оценка корректности назначенных прав доступа остаётся сложной и непрозрачной задачей. Проблема усугубляется тем, что чрезмерные привилегии, известные как избыточные разрешения (over-permissioning), не всегда очевидны при ручном анализе и могут предоставлять злоумышленнику неожиданные возможности для эскалации привилегий внутри кластера.

Основная сложность заключается в высокой связности и многоуровневости объектов RBAC. В крупном кластере с десятками сервисных аккаунтов, ролей и привязок ручной аудит становится практически невыполнимой задачей, подверженной ошибкам. Аналитика необходимо не просто изучить отдельные манифесты, а понять полную картину распределения прав: какой субъект и при каких условиях получает доступ к конкретному ресурсу. Это создаёт значительные трудности при моделировании действий потенциального злоумышленника и выявлении неочевидных векторов атак, например возможности использования технических аккаунтов для обхода установленных ограничений [2].

Полученные результаты анализа полезны не только для поиска уязвимостей в ходе тестирования на проникновение, но и для построения систематических методик защиты [3]. На основе выявленных зависимостей можно формировать политики минимально необходимых прав, исключать избыточные роли и оптимизировать архитектуру доступа ещё до момента эксплуатации. Кроме того, анализ поведения системы через журналы аудита позволяет выявлять попытки несанкционированного использования прав и корректировать конфигурацию до того, как уязвимость будет реализована на практике [4, 5]. Таким образом, аудит RBAC становится не разовой проверкой, а основой для постоянного повышения уровня безопасности.

Для повышения полноты анализа всё чаще используются инструменты, работающие с журналами и событиями Kubernetes. Средства наподобие kubeaudit или kubectl-who-can позволяют автоматизировать проверку политик и выявлять скрытые зависимости, которые трудно обнаружить вручную. Важным дополнением является корреляция событий в логах API-сервера: отслеживание последовательности запросов помогает понять, как конкретные разрешения используются в реальной среде, и обнаружить нетипичные сценарии доступа. Такой подход делает аудит более объективным и позволяет выявлять векторы атак, заложенные не только в конфигурациях, но и в фактическом поведении системы. Это смещает акцент с поиска локальных ошибок на анализ устойчивости кластера к целенаправленным атакам.

### СПИСОК ЛИТЕРАТУРЫ

1. Malkov E.V., Ananchenko I.V. Analysis of dac, rbac, abac: advantages, disadvantages, approaches to selection // Актуальные вопросы современных научных исследований. 2025. С. 77-81.
2. Rostami G., Role-Based Access Control (RBAC) Authorization in Kubernetes//Journal of ICT Standardization. 2023. Vol. 11, no. 3. Pp. 237-260.
3. Islam Shamim M.S., Ahamed Bhuiyan F., Rahman A. XI Commandments of Kubernetes Security: A Systematization of Knowledge Related to Kubernetes Security Practices//2020 IEEE Secure Development (SecDev). 2020. Pp. 58-64.
4. Шариков, П. И. Архитектура интегрированного java-приложения для анализа журналов с целью обнаружения компьютерных атак в информационных системах посредством реагирования на различные аномалии безопасности / П. И. Шариков, А. В. Красов, А. В. Майоров // Вестник Дагестанского государственного технического университета. Технические науки. 2025. Т. 52, № 1. С. 147-161. DOI 10.21822/2073-6185-2025-52-1-147-161. EDN AWEHRP.
5. Дудников, И. А. Методика анализа журналов событий информационных систем с использованием Elasticsearch для обнаружения сигналов о вредоносных действиях в информационной системе / И. А. Дудников, П. И. Шариков, А. В. Майоров // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2025. № 1. С. 120-134. DOI 10.61260/2218-130X-2025-1-120-134. EDN ZQCEXG.

УДК 658.64

## МЕТОДЫ СТАТИЧЕСКОГО АНАЛИЗА ДЛЯ ВЫЯВЛЕНИЯ ДЕФЕКТОВ И УЛУЧШЕНИЯ ЧИСТОТЫ КОДА

**Орлова Дарья Алексеевна**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mail: dashhhhhhhh\_ka@mail.ru

**Аннотация.** В работе проведено исследование эффективности применения методов статического анализа для повышения качества программного кода. Рассмотрены основные подходы к анализу кода, их преимущества и ограничения. Приведены результаты практического применения инструментов статического анализа в российских ИТ-проектах, показавшие значительное снижение плотности дефектов и времени на код-ревью. Особое внимание уделено интеграции статического анализа в процессы разработки и его влиянию на ключевые метрики кода, такие как цикломатическая сложность и технический долг.

**Ключевые слова:** статический анализ; качество кода; метрики кода; инструменты анализа; PVS-Studio; ошибки в ПО; технический долг; стандарты кодирования.

## STATIC ANALYSIS METHODS FOR IDENTIFYING DEFECTS AND IMPROVING CODE CLEANLINESS

**Orlova Daria**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications  
22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mail: dashhhhhhhh\_ka@mail.ru

**Abstract.** The paper investigates the effectiveness of static analysis methods for improving code quality. The main approaches to code analysis, their advantages and limitations are considered. The results of practical application of static analysis tools in Russian IT projects are presented, showing a significant reduction in defect density and code review time. Particular attention is paid to the integration of static analysis into development processes and its impact on key code metrics, such as cyclomatic complexity and technical debt.

**Keywords:** static analysis; code quality; code metrics; analysis tools; PVS-Studio; software errors; technical debt; coding standards.

Современные программные системы характеризуются высокой сложностью и требовательностью к надежности. По данным исследования ИСП РАН, до 40% затрат на разработку приходится на исправление дефектов, которые могли быть выявлены на этапе написания кода [1]. Традиционные методы контроля качества, такие как ручной код-ревью и динамическое тестирование, обладают существенными ограничениями: высокая трудоемкость и позднее обнаружение ошибок. В связи с этим статический анализ кода, выполняемый без запуска программы, становится критически важным инструментом для выявления дефектов, уязвимостей и нарушений стандартов кодирования на ранних стадиях жизненного цикла ПО.

Проанализированы ключевые методы статического анализа, применяемые в современных инструментах: анализ потока данных, символьное выполнение, паттерн-ориентированный и метрический анализ [3]. Показано, что их комбинированное применение позволяет выявлять до 45% логических ошибок и 25% утечек ресурсов на ранних этапах разработки [2]. Эффективность статического анализа подтверждена результатами внедрения в российских ИТ-проектах. На примере проекта «Ростелеком» продемонстрировано, что внедрение инструмента PVS-Studio позволило снизить плотность дефектов с 1.5 до 0.7 на 1000 строк кода и сократить время код-ревью на 40% [1]. Цикломатическая сложность кода в проекте «Ростелеком» снизилась с 50 до 32, а количество блокирующих дефектов — с 25 до 5, что свидетельствует о значительном улучшении читаемости и управляемости кода [3]. В одном из ведущих российских банков внедрение SonarQube способствовало сокращению технического долга на 35% и повышению соответствия стандарту MISRA-C с 70% до 92% [5].

Несмотря на эффективность, использование инструментов статического анализа сопряжено с проблемами, такими как ложные срабатывания (до 20% для PVS-Studio) и высокий порог входа [4]. Для повышения эффективности предлагаются рекомендации: кастомизация правил анализа для снижения уровня шума, поэтапное внедрение с началом в тестовом режиме, комбинирование инструментов для многоязычных проектов и регулярный анализ метрик для оценки прогресса [2].

Таким образом, методы и инструменты статического анализа кода демонстрируют высокую эффективность в повышении качества программного обеспечения, снижении технического долга и оптимизации процессов разработки. Их внедрение позволяет существенно улучшить ключевые метрики кода и сократить затраты на исправление ошибок. Для достижения оптимальных результатов необходимы корректная настройка инструментов, их глубокая интеграция в процессы разработки, обучение команд и акцент на ключевых метриках.

## СПИСОК ЛИТЕРАТУРЫ

1. Бударный, Г. С. Сравнение статического и динамического анализа кода и их роль в методологии devsecops / Г. С. Бударный, А. О. Камалова, А. В. Красов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): Сборник научных статей. XII Международная научно-техническая и научно-методическая конференция. В 4 т., Санкт-Петербург, 28 февраля – 01 марта 2023 года. Том 1. СПб.: СПбГУ телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2023. С. 204-208. EDN KAUWLG.

2. Бударный, Г. С. Сравнение методов статического анализа исходного кода программы / Г. С. Бударный, И. Е. Пестов, И. Г. Штеренберг // Вестник СПбГУПТД. Серия 1: Естественные и технические науки. 2024. № 1. С. 5-12. DOI 10.46418/2079-8199\_2024\_1\_1. EDN QNAQJJ.
3. Алехин, Р. В. Статистические методы анализа данных / Р. В. Алехин, Г. С. Бударный, А. О. Камалова // Студенческая весна - 2024: Сборник научных статей 78-ой региональной научно-технической конференции студентов, аспирантов и молодых ученых, Санкт-Петербург, 15 мая 2024 года. СПб: СПбГУ телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2024. С. 53-57. EDN HZDTTS.
4. Дудников, И. А. Методика анализа журналов событий информационных систем с использованием Elasticsearch для обнаружения сигналов о вредоносных действиях в информационной системе / И. А. Дудников, П. И. Шариков, А. В. Майоров // Научно-аналитический журнал Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. 2025. № 1. С. 120-134. DOI 10.61260/2218-130X-2025-1-120-134. EDN ZQCEXG.
5. Шариков, П. И. Методика обфускации байт-кода Java-приложения с целью его защиты от атак декомпиляцией / П. И. Шариков // Вестник СПбГУПТД. Серия 1: Естественные и технические науки. 2022. № 1. С. 64-72. DOI 10.46418/2079-8199\_2022\_1\_10. EDN AUOFNA.

УДК 004.056

## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИОТ В СЕТЯХ 6G

**Пивоваров Даниил Сергеевич, Тимофеев Лавр Алексеевич, Шевченко Александр Александрович**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

e-mails: Pivovarov.danya@yandex.ru, other.saew@mail.ru, alex\_pavel1991@mail.ru

**Аннотация.** В работе рассматриваются ключевые угрозы безопасности, возникающие при интеграции устройств Интернета вещей в инфраструктуру 6G. Подчеркивается роль архитектур SDN, NFV и MEC в наследовании уязвимостей от предыдущего поколения, а также влияние экспоненциального роста IoT на расширение поверхности атак. Анализируются риски, связанные с низкой защищённостью устройств, их разнообразием и ограниченными ресурсами, а также угрозы конфиденциальности при обработке больших массивов данных. Представлены результаты моделирования DDoS-атаки на контроллер SDN, подтверждающие необходимость комплексных мер защиты.

**Ключевые слова:** 6G; IoT; киберугрозы; уязвимости; безопасность; DDoS.

## IOT INFORMATION SECURITY IN 6G NETWORKS

**Pivovarov Daniil, Timofeev Lavr, Shevchenko Aleksandr**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

22 Bolshevnikov Av, bldg 1, St. Petersburg, 193232, Russia

e-mails: Pivovarov.danya@yandex.ru, other.saew@mail.ru, alex\_pavel1991@mail.ru

**Abstract.** This study explores major security threats emerging from the integration of Internet of Things devices into 6G infrastructures. It emphasizes the role of SDN, NFV, and MEC in inheriting vulnerabilities from previous generations, as well as the impact of IoT's exponential growth on the expansion of attack surfaces. Risks associated with weak device protection, resource limitations, and data privacy threats are analyzed. Simulation results of a DDoS attack on an SDN controller highlight the need for comprehensive defense strategies.

**Keywords:** 6G; IoT; cyber threats; vulnerabilities; security; DDoS.

Развитие мобильной связи шестого поколения открывает принципиально новые возможности для цифровой трансформации общества. Сверхнизкие задержки, высокая пропускная способность и поддержка огромного количества подключений обеспечивают основу для создания умных городов, цифровой промышленности и интеллектуальных систем здравоохранения. Однако наряду с перспективами возникают масштабные вызовы в области информационной безопасности [1–4].

Сети 6G формируются не на пустом месте, а наследуют архитектурные принципы 5G, включая SDN, NFV и MEC. Эти технологии обеспечивают гибкость и эффективность управления сетью, но одновременно создают точки уязвимости. Централизованные контроллеры SDN становятся критически важными объектами для злоумышленников, атака на которые может привести к полной компрометации сети. Виртуализация сетевых функций на базе NFV повышает риск компрометации гипервизора и нарушения изоляции виртуальных машин. Серверы MEC, размещаемые на периферии, оказываются подвержены как сетевым, так и физическим атакам, что делает их особенно уязвимыми в распределенной инфраструктуре [5–7].

Существенно усложняет ситуацию экспоненциальное увеличение числа IoT-устройств, подключаемых к сетям 6G. Многие из них имеют ограниченные ресурсы и не способны реализовать сложные механизмы защиты. Производители часто уделяют недостаточное внимание вопросам безопасности, поставляя устройства с уязвимыми настройками по умолчанию, отсутствием обновлений и слабой защитой коммуникационных каналов. Это превращает IoT в удобную точку входа для киберпреступников [8–10].

Разнообразие IoT-экосистемы также приводит к невозможности создания универсальной модели защиты. Злоумышленники получают возможность использовать устройства как для атак на пользователей и кражи данных, так и для формирования ботнетов, задействованных в масштабных DDoS-кампаниях. Атаки на цепочку поставок дополняют спектр угроз, позволяя внедрять уязвимые компоненты еще на этапе производства [11].

Не менее актуальной становится проблема конфиденциальности. IoT-устройства собирают колоссальные объемы информации о повседневной жизни пользователей — от данных о местоположении до параметров

здоровья. Недостаточная защита этих данных создает угрозы шантажа, мошенничества и слежки. Массовый сбор и анализ информации открывают возможности для скрытого профилирования и манипуляций [12–14].

Проведенное моделирование DDoS-атаки на контроллер SDN подтверждает, что даже ограниченная по масштабу атака способна вызвать перегрузку сети и вывести из строя критические сервисы. Это доказывает необходимость перехода к комплексным стратегиям защиты, включающим проектирование безопасных IoT-устройств, усиление механизмов сетевой безопасности, применение методов искусственного интеллекта для обнаружения атак и разработку систем адаптивного реагирования.

Формирование надежной инфраструктуры 6G требует внимания не только к техническим решениям, но и к правовым аспектам. Необходима разработка единых стандартов и нормативов, регулирующих защиту данных и эксплуатацию IoT-устройств. Только интеграция инновационных технологий с продуманной законодательной базой позволит создать устойчивую и безопасную экосистему 6G, способную обеспечить доверие пользователей и устойчивое развитие цифрового общества.

#### СПИСОК ЛИТЕРАТУРЫ

1. Бужин, И. Г. Особенности классификации и фильтрации трафика сети передачи данных 6G / И. Г. Бужин, В. М. Антонова, Ю. Б. Мионов [и др.] // Труды МАИ. 2021. № 121. URL: <https://cyberleninka.ru/article/n/osobennosti-klassifikatsii-i-filtratsii-trafika-seti-peredachi-dannyh-6g> (дата обращения: 25.04.2025).
2. Ефременко, В. Безопасность 6G и IoT: какие угрозы перейдут из 5G и как им противостоять / В. Ефременко // Хабр. URL: <https://habr.com/ru/companies/selectel/articles/793196/> (дата обращения: 25.04.2025).
3. Пахаев, Х. Х. Обзор угроз безопасности интернета вещей / Х. Х. Пахаев, Т. Г. Айгунов, Э. М. Абдулмукуминова // ИВД. 2022. № 10 (94). URL: <https://cyberleninka.ru/article/n/obzor-ugroz-bezopasnosti-interneta-veschey> (дата обращения: 25.04.2025).
4. Минаев, В. А. Безопасность Интернета вещей: основные решения / В. А. Минаев, Б. А. Швырев, Т. Р. Ромашкин // Информация и безопасность. 2023. Т. 26, № 2. С. 163–168. DOI: 10.36622/VSTU.2023.26.2.001. ISSN: 1682-7813.
5. Gilchrist, A. IoT Security: An End-to-End Perspective / A. Gilchrist. Boca Raton : CRC Press, 2017. 350 p. ISBN: 978-1-4987-6157-4.
6. Abbas, N. A Survey on Security for Mobile Edge Computing / N. Abbas, Y. Zhang, Q. T. Dinh, T. A. T. Nguyen // IEEE Communications Surveys & Tutorials. 2018. Vol. 20, № 4. P. 2855-2885. DOI: 10.1109/COMST.2018.2844168.
7. Gharbaoui, M. Security in Network Functions Virtualization: A Survey / M. Gharbaoui, M. Debbabi, A. Belguith, L. Khoukhi // IEEE Communications Surveys & Tutorials. 2016. Vol. 18, No. 4. P. 2556-2584. DOI: 10.1109/COMST.2016.2581821.
8. Лобова, А. И. Обзор DDoS-атак на IoT устройства / А. И. Лобова, Е. В. Вершинин, В. О. Фёдоров // Нацбезопасность. 2022. № 1 (3). URL: <https://cyberleninka.ru/article/n/obzor-ddos-atak-na-iot-ustroystva> (дата обращения: 26.04.2025).
9. Липатников В.А., Шевченко А.А. Модель процесса управления информационной безопасностью распределенной информационной системы на основе выявления и оценки уязвимостей // Информационные системы и технологии. 2018. № 1(105). С. 114-123.
10. Липатников В.А., Шевченко А.А. Проактивное управление информационной безопасностью автоматизированной системы радиоконтроля // Информационные системы и технологии. 2019. № 4(114). С. 112-121.
11. Липатников В.А., Ложечкин А.А., Шевченко А.А. Построение комплексной защиты киберфизической системы от деструктивных воздействий // Информационные системы и технологии. 2020. № 6(122). С. 112-120.
12. Билятдинов, К. З. Исследование систем и анализ результатов испытаний / К. З. Билятдинов, А. В. Красов, В. В. Меняйло СПбГУ телекоммуникаций им. проф. М.А. Бонч-Бруевича. Санкт-Петербург : Центр научно-информационных технологий «Астерион», 2019. 362 с. ISBN 978-5-00045-813-6. EDN OXKBZW.
13. Миняев, А. А. Методика оценки эффективности системы защиты информации территориально-распределенных информационных систем / А. А. Миняев, А. В. Красов // Вестник СПбГУПТД. Серия 1: Естественные и технические науки. 2020. № 3. С. 26-32. DOI 10.46418/2079-8199\_2020\_3\_4. EDN YNHOEI.
14. Yurkin, D. V. Formation of the instantaneous information security audit concept / D. V. Yurkin, I. I. Livshitz, A. A. Minyaev // Communications in Computer and Information Science. 2016. Vol. 678. P. 314-324. DOI 10.1007/978-3-319-51917-3\_28. EDN YVGPXZ.

УДК 004.057.8

#### ИССЛЕДОВАНИЕ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ КАК ТЕХНОЛОГИИ ДЛЯ АВТОМАТИЗИРОВАННОГО РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ

**Платонов Алексей Евгеньевич, Ковзур Максим Михайлович, Миняев Андрей Анатольевич**  
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевики пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mails: alexeyplatonov53@gmail.com, maxkovzur@mail.ru, minyaev1.a@sut.ru

**Аннотация.** Современные системы обеспечения информационной безопасности позволяют автоматизировать работу по выявлению и противодействию кибератакам. Обзор применимости данной технологии для автоматизации реагирования на инциденты, их расследования и предотвращения даст понимание того, в каких сферах информационной безопасности их лучше всего применять

**Ключевые слова:** большие языковые модели; SOAR; информационная безопасность.

#### RESEARCH OF NEURAL NETWORK TECHNOLOGIES AS A TECHNOLOGY FOR AUTOMATED INCIDENT RESPONSE

**Platonov Aleksei, Kovzur Maxim, Minyaev Andrei**  
The Bonch-Bruevich Saint Petersburg State University of Telecommunications  
22 Bolshhevikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mails: alexeyplatonov53@gmail.com, maxkovzur@mail.ru, minyaev.a@gmail.com

**Abstract.** Modern information security systems make it possible to automate the work to identify and counter cyberattacks. An overview of the applicability of this technology for automating incident response, investigation, and prevention will provide an understanding of which areas of information security are best used

**Keywords:** large language models; laboratory stand; cyber security.

В течение 2024 года, количество пострадавших от кибератак превысило 1,6 миллиард человек [1], причем по сравнению с предыдущими периодами, количество атак только растет. Одним из решений по противодействию увеличенного количества атак и упрощению работ по информационной безопасности является автоматизация процессов анализа, мониторинга и противодействия атакам, посредством использования систем информационной безопасности.

Одной из проблем для работников SOC (Security Operation Center) [2] — центров, является большое количество рутинных задач и типовой информации, которая требует концентрации внимания и может замедлить реакцию на более важные события, происходящие в информационной системе.

Современные системы обеспечения информационной безопасности обрабатывают огромное количество информации, поступающей с устройств. Для облегчения работы SOC-центров, были разработаны SOAR (Security Orchestration, Automation and Response) [3] — системы, которые позволяют автоматизировать рутинные процессы анализа данных, и позволяют работникам фокусировать внимание на более важные задачи, требующие вмешательства человека.

С развитием больших языковых моделей, возникает все больше возможностей по их интеграции в рабочие процессы и системы информационной безопасности. Обработывая журналы событий, большие языковые модели могут выделять ценную информацию, и представлять ее в удобочитаемом виде, помогая работникам определить причины, следствия и порядок событий, происходящих в системе [4].

Обзор данных технологий в ключе применимости для автоматизации работы SOC-центров позволяет определить применимость больших языковых моделей для этих целей. Определяются основные задачи, поставленные перед центрами SOC и SOAR-системами, исследуется применимость больших языковых моделей для этих областей.

Целью авторов является оценка качества детектирования атак разными большими языковыми моделями, их способность анализировать и представлять результаты анализа.

#### СПИСОК ЛИТЕРАТУРЫ

1. How Many Cyber Attacks Occur Each Day? [Электронный ресурс]. 2025. Режим доступа: <https://explodingtopics.com/blog/cybersecurity-stats> (дата обращения: 21.08.2025).
2. SOC (Security Operation Center): что это такое и зачем используется? Центры мониторинга информационной безопасности [Электронный ресурс]. Режим доступа: <https://www.securityvision.ru/blog/soc-cto-eto/> (дата обращения: 21.08.2025).
3. SOAR (Security Orchestration, Automation and Response) [Электронный ресурс]. Режим доступа: <https://encyclopedia.kaspersky.ru/glossary/security-orchestration-automation-and-response-soar/> (дата обращения: 21.08.2025).
4. Ковцур М. М., Ахrameeva К. А., Зебзеев Е. А., Пронин В. Д. Определение применяемых протоколов информационной безопасности беспроводной сети на основе дампа трафика // Наука и образование в условиях мировой нестабильности: проблемы, новые этапы развития: материалы II Международной научно-практической конференции. Ростов-на-Дону: Национальный исследовательский институт дополнительного профессионального образования, 2022. С. 119–123.

УДК 004.056.53

### ИНТЕГРАЦИЯ КОНЦЕПЦИЙ «УМНОГО ПРОИЗВОДСТВА» И КИБЕРБЕЗОПАСНОСТИ В АСУ ТП

**Повышев Сергей Алексеевич, Штеренберг Станислав Игоревич**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

Большевикова пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

e-mails: SPovyshev@phosagro.ru, shterenberg.stanislaw@yandex.ru

**Аннотация.** В тезисе показано исследование подходов к интеграции IoT-устройств и больших данных в АСУ ТП, а также обсуждение связанных с этим рисков и необходимых мер безопасности для защиты данных и технологических процессов. Также имеет место изучение существующих стандартов и нормативных актов и их применение для повышения уровня защиты информационной инфраструктуры химических предприятий. Рассмотрение современных методов выявления и предотвращения кибератак на АСУ ТП, включая использование систем обнаружения вторжений (IDS), шифрование данных и применение безопасных архитектур позволяет зафиксировать сценарии реальных случаев кибератак на предприятия химической промышленности, анализ причин и последствий.

**Ключевые слова:** химическая промышленность; АСУТП; 187-ФЗ; КСПД; риски ИБ; КИИ.

### INTEGRATION OF SMART MANUFACTURING AND CYBERSECURITY CONCEPTS INTO AUTOMATED PROCESS CONTROL SYSTEMS

**Pozishev Sergey, Shterenberg Stanislav**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

22 Bolshevnikov Av, bldg 1, St. Petersburg, 193232, Russia

e-mails: SPovyshev@phosagro.ru, shterenberg.stanislaw@yandex.ru

**Abstract.** The thesis shows a study of approaches to integrating IoT devices and big data into automated process control systems, as well as a discussion of the associated risks and necessary security measures to protect data and technological processes. There is also a study of existing standards and regulations and their application to increase the

level of protection of the information infrastructure of chemical enterprises. Consideration of modern methods for detecting and preventing cyber-attacks on automated process control systems, including the use of intrusion detection systems (IDS), data encryption and the use of secure architecture allows us to capture scenarios of real cases of cyber-attacks on chemical industry enterprises, and analyze the causes and consequences.

**Keywords:** chemical industry; automated control systems; enterprise protection; corporate network; information security incidents; emergency situations.

В условиях роста угроз и сложностей, связанных с эксплуатацией объектов химической промышленности, проблема безопасности становится особенно актуальной. Данная работа посвящена интеграции цифровых двойников в системы мониторинга и управления рисками на химических предприятиях. Цифровые двойники, представляющие собой виртуальные модели физических объектов, позволяют в реальном времени отслеживать состояние оборудования, прогнозировать возможные аварийные ситуации и оптимизировать процессы управления. В докладе рассматриваются современные подходы к созданию в том числе и цифровых двойников, их роль в повышении уровня безопасности, а также примеры успешного внедрения в промышленности. Оценка эффективности данного решения позволит не только минимизировать риски, но и улучшить общую производительность и устойчивость объектов химической промышленности [1, 2].

Цель — установка требований и рекомендаций, предъявляемые к разработчикам, которые необходимы для обеспечения информационной безопасности и защиты интересов заказчика при использовании подрядчиками информационных активов предприятия [3–5]. Выполнив категорирование, предприятие получает четкое понимание, какие свои системы следует считать критически важными и защищать в приоритетном порядке. Кроме того, выполнение требований закона — залог отсутствия правовых санкций. За нарушение обязанностей 187-ФЗ предусмотрена ответственность, вплоть до штрафов и даже уголовных дел (например, ст. 274.1 УК РФ за неправомерное воздействие на критическую инфраструктуру). Но главным стимулом должна быть не боязнь наказания, а осознание, что адекватная защита, в том числе и АСУТП, минимизирует риски тяжелых техногенных аварий и сбоев производства.

Эффективное управление рисками на объектах критической информационной инфраструктуры (КИИ) требует не только разработки математических моделей оценки угроз, но и их наглядной визуализации, интеграции в интерфейс пользователя и практического применения в системах поддержки принятия решений [6–8]. В условиях территориальной распределённости объектов на химическом предприятии, разнородности угроз и необходимости учёта множества факторов (в том числе экзогенных) особую значимость приобретает геоинформационный подход, сочетающий в себе пространственный анализ, прогнозные модели и формализованные оценки значимости [9, 10]. Наиболее перспективным направлением может быть гибридная модель, сочетающая сильные стороны синхронной и асинхронной репликации и демонстрирующая высокую степень адаптивности в условиях нестабильной нагрузки и критически важных задач [11, 12].

#### СПИСОК ЛИТЕРАТУРЫ

1. Проничев, В. Д. Автоматизированный анализ изменений в сетевых конфигурациях устройств на основе нейронных сетей / В. Д. Проничев, И. А. Ушаков // Подготовка профессиональных кадров в магистратуре в эпоху цифровой трансформации (ПКМ-2024) : Сборник лучших докладов V Всероссийской научно-технической и научно-методической конференции магистрантов и их руководителей. В 2-х томах, Санкт-Петербург, 03–05 декабря 2024 года. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2025. С. 443–448. EDN DDZZOT.
2. Анализ современных средств автоматизированной проверки функций безопасности коммутационного оборудования / П. В. Карельский, М. М. Ковцур, С. И. Штеренберг, Н. И. Малинин // Информационная безопасность регионов России (ИБРР-2021) : Материалы XII Санкт-Петербургской межрегиональной конференции, Санкт-Петербург, 27–29 ноября 2021 года. СПб.: СПОИСУ, 2021. С. 385–386.
3. Аксенов, К. Д. Защита медицинских данных в эпоху развития технологий искусственного интеллекта / К. Д. Аксенов, А. В. Красов // Региональная информатика (РИ-2024) : Материалы XIX Санкт-Петербургской международной конференции, Санкт-Петербург, 23–25 октября 2024 года. СПб.: СПОИСУ, 2024. С. 89–90. EDN ASDYIF.
4. Ушаков, И. А. Обзор сетевых индикаторов компрометации для обнаружения каналов управления вредоносным программным обеспечением / И. А. Ушаков, М. А. Скорых // 65-я научно-техническая конференция профессорско-преподавательского состава, научных работников и аспирантов (НТК ППС 2025) : Сборник научных статей. В 3 т., Санкт-Петербург, 17–21 февраля 2025 года. СПб.: СПбГУ телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2025. С. 500–505. EDN RNIDSX.
5. Красов, А. В. Использование IP UATC Agat CU в условиях импортозамещения / А. В. Красов, А. В. Поляничева, А. И. Сафина // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023) : Сборник научных статей. XII Международная научно-техническая и научно-методическая конференция. В 4 т., Санкт-Петербург, 28 февраля 01 марта 2023 года. Том 1. СПб.: СПбГУ телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2023. С. 711–715. EDN DGDOXB.
6. Research and Evaluation of the Most Significant Quantitative Characteristics of MPLS Equipment / A. Krasov, P. Karelsky, I. Zuyev [et al.] // Smart Innovation, Systems and Technologies. 2021. Vol. 220. P. 431–443. DOI 10.1007/978-981-33-6632-9\_38. EDN KHZCLM.
7. Тетеркин В. Ф., Митрошин А. А., Чернышев С. В. Регламент сопровождения межсетевого экрана, сертифицированного ФСТЭК // Материалы Международной научно-практической конференции по обеспечению комплексной безопасности предприятий: проблемы и решения. 2015. С. 95.
8. Крутиков, А. Н. Методы обнаружения инсайдеров в компьютерных сетях с использованием больших данных / А. Н. Крутиков, В. А. Страйстар, И. А. Ушаков // Актуальные проблемы инфотелекоммуникаций в науке и образовании : Сборник научных статей XIII Международной научно-технической и научно-методической конференции в 4 т., Санкт-Петербург, 27–28 февраля 2024 года. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2024. С. 507–510. EDN OHMPGB.
9. Проничев, В. Д. Разработка модели инсайдера в компьютерных сетях / В. Д. Проничев, И. А. Ушаков // Актуальные проблемы инфотелекоммуникаций в науке и образовании : Сборник научных статей XIII Международной научно-технической и научно-методической конференции в 4 т., Санкт-Петербург, 27–28 февраля 2024 года. СПб.: СПбГУ телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2024. С. 602–605. EDN BAVZPQ.

10. Штеренберг, С. И. Архитектура защищенной интеллектуальной системы обнаружения вторжений и инцидентов в распределенных информационных системах / С. И. Штеренберг // Региональная информатика и информационная безопасность : Сборник трудов Санкт-Петербургской международной конференции, Санкт-Петербург, 25–27 октября 2023 года. Санкт-Петербург: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2023. С. 321–326. EDN IIZFPV.
11. Оценка статистических характеристик различных типов фреймов IEEE 802.11 для сервисов местоположения / В. А. Петров, М. М. Ковцур, А. Ю. Киструга, С. И. Штеренберг // Информационная безопасность регионов России (ИБРР-2021) : Материалы XII Санкт-Петербургской межрегиональной конференции, Санкт-Петербург, 27–29 ноября 2021 года. СПб.: СПОИСУ, 2021. С. 187–188. EDN NNCOMDY.
12. Ушаков, И. А. Обоснование демаскирующих признаков инсайдеров в корпоративных компьютерных сетях / И. А. Ушаков // Вестник СПбГУПТД. Серия 1: Естественные и технические науки. 2024. № 3. С. 95–106. DOI 10.46418/2079-8199\_2024\_3\_15. EDN JADZTQ.

УДК 004.021

## КОНЕЧНЫЕ АВТОМАТЫ В СИСТЕМАХ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ: ФОРМАЛИЗАЦИЯ ПОВЕДЕНИЯ ДЛЯ АНАЛИЗА АНОМАЛИЙ В LINUX-СРЕДАХ

Потемкина Юлия Фёдоровна

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mail: julia.potemkina24@yandex.ru

**Аннотация.** Данная статья посвящена применению конечных автоматов как формального математического инструмента для моделирования и анализа нормального и аномального поведения в системах обнаружения вторжений.

**Ключевые слова:** поведенческий анализ; обнаружение аномалий; конечный автомат; аутентификация; auditd; анализ логов; информационная безопасность; Linux.

## BEHAVIORAL MODELING WITH FINITE AUTOMATA IN INTRUSION DETECTION SYSTEMS: SEMANTIC ANALYSIS OF SYSTEM EVENTS IN LINUX ENVIRONMENTS

Potemkina Yuliya

The Bonch-Bruevich Saint Petersburg State University of Telecommunications  
22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mail: julia.potemkina24@yandex.ru

**Abstract.** This article is devoted to the use of finite automata as a formal mathematical tool for modeling and analyzing normal and abnormal behavior in intrusion detection systems.

**Keywords:** behavioral analysis; anomaly detection; finite state machine; authentication; auditd; log analysis; information security; Linux.

Системы обнаружения вторжений (IDS) традиционно полагались на сигнатурный анализ — сравнение сетевого или системного трафика с заранее определёнными шаблонами известных атак. Однако современные угрозы, такие как целенаправленные атаки с длительным присутствием, адаптивные брутфорс-атаки и атаки «внутри сети», часто используют легитимные инструменты и манипулируют порядком операций, что делает их невидимыми для сигнатурных методов [1].

Для преодоления этих ограничений активно развиваются подходы, основанные на поведенческом анализе, где ключевым элементом становится моделирование нормального поведения системы и выявление отклонений от него. Одним из наиболее эффективных и формально обоснованных инструментов для такого моделирования являются конечные автоматы — математические абстракции, способные описывать дискретные состояния системы и детерминированные переходы между ними под воздействием внешних событий [2].

В данной работе исследуется возможность использования конечных автоматов как основы для построения высокоточных IDS в среде Linux, где источником данных служит ядерный аудит через auditd. В отличие от других методов машинного обучения, требующих больших объёмов данных и сложной настройки, конечные автоматы обеспечивают интерпретируемость, воспроизводимость и минимальную сложность реализации, что особенно важно для критически важных инфраструктур.

Для формализации и анализа поведения в условиях, где важна последовательность событий, широкое применение находят модели конечных автоматов [3]. Конечный автомат — это математическая модель вычислений, представляемый как кортеж  $M = (Q, \Sigma, \delta, q_0, F)$ , где  $Q$  — конечное множество состояний,  $\Sigma$  — входной алфавит (множество событий),  $\delta: Q \times \Sigma \rightarrow Q$  — функция переходов,  $q_0 \in Q$  — начальное состояние,  $F \subseteq Q$  — множество конечных (допускающих) состояний.

В контексте IDS, каждое состояние  $qi \in Q$  соответствует определённому этапу жизненного цикла пользователя или процесса в системе, а переходы инициируются событиями, генерируемыми ядром Linux через auditd.

Для построения достоверных моделей поведения необходим источник событий, обладающий высокой детализацией, целостностью и защитой от манипуляций — именно такие характеристики обеспечивает утилита auditd, интегрированная на уровне ядра Linux. Она фиксирует системные вызовы в реальном времени, привязывая каждое событие к уникальным атрибутам: аудит-идентификатору пользователя, идентификатору процесса, сетевому адресу источника подключения и точной временной метке, что позволяет однозначно восстанавливать контекст действий. Логи собираются в защищённый файл /var/log/audit/audit.log, который может

быть переведён в режим неизменности, исключая возможность удаления или модификации записей даже при компрометации пользовательской среды. В отличие от традиционных механизмов журналирования, таких как syslog, auditd не полагается на пользовательские демоны и предоставляет возможность фильтрации событий по их семантическому типу — будь то попытки аутентификации, запуск исполняемых файлов, вход в сессию или системные вызовы — обеспечивая тем самым непрерывность и надёжность сбора данных вне зависимости от состояния прикладного уровня. Благодаря этой глубине и устойчивости к вмешательству, auditd становится основой для формирования детерминированных и воспроизводимых моделей поведения, свободных от искажений, вызванных ошибками программного обеспечения или активностью злоумышленника. На практике логи auditd преобразуются в поток дискретных событий, которые затем анализируются и классифицируются как символы алфавита  $\Sigma$ . Каждый поток, соответствующий отдельной пользовательской сессии, рассматривается как строка над этим алфавитом, которая должна быть распознана конечным автоматом как элемент регулярного языка, описывающего нормальное поведение системы.

В контексте анализа аутентификации каждое состояние конечного автомата может соответствовать определённому этапу жизненного цикла сессии: попытка входа, проверка учётной записи, инициализация сессии, успешный вход, неудачная аутентификация и активная работа в системе. Переходы между состояниями инициируются событиями, зафиксированными в логах auditd. Построение модели нормального поведения сводится к определению допустимых последовательностей переходов, типичных для легитимных пользователей. Аномалия распознаётся как появление недопустимых переходов, циклических петель (например, многократное возвращение к попытке входа после неудачи), отсутствие логического завершения сессии или существенное отклонение от вероятностного распределения переходов, выявленного в ходе обучения модели.

Таким образом, комбинация глубокого системного аудита с помощью auditd, поведенческого анализа и формального моделирования на основе конечных автоматов образует мощную теоретическую основу для построения эффективных систем обнаружения вторжений. Подход позволяет перейти от реактивного анализа отдельных событий к проактивному выявлению отклонений в поведении, основанных на логической и временной структуре взаимодействий. Он обеспечивает высокую степень формализации, воспроизводимости и потенциал для автоматизации, что делает его перспективным направлением в области поведенческой аналитики и обеспечения безопасности операционных систем.

#### СПИСОК ЛИТЕРАТУРЫ

1. Сбор и анализ логов в Linux [Электронный ресурс]: HABR.COM. URL: <https://habr.com/ru/companies/otus/articles/714266/> (дата обращения: 10.08.2025).
2. Едемская, Е. Д. Использование auditd для логирования в Linux системах / Е. Д. Едемская, В. В. Пучков // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023) : Сборник научных статей. XII Международная научно-техническая и научно-методическая конференция. В 4 т., Санкт-Петербург, 28 февраля 01 марта 2023 года. Том 1. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2023. С. 438-443. EDN OWAMGG.
3. Любимова, Т. В. Конечный автомат: теория и реализация / Т. В. Любимова // Университетская наука. 2020. № 1(9). С. 117-121. EDN XUNYDC.

УДК 004.056

### СОВРЕМЕННЫЕ ВЕКТОРЫ РАЗВИТИЯ СИСТЕМ КОНТРОЛЯ ДОСТУПА В ВЕБ-ПРИЛОЖЕНИЯХ

Рогатых Ксения Александровна

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевики пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mail: kseniarogatyh@yandex.ru

**Аннотация.** В тезисах рассматриваются эволюция и ключевые направления совершенствования механизмов аутентификации и авторизации как фундамента безопасности веб-приложений. Анализируется переход от традиционных методов к многофакторным и биометрическим подходам, а также к децентрализованным моделям авторизации. Особое внимание уделяется комплексному противодействию современным киберугрозам через интеграцию технологий и протоколов. Определены перспективные тенденции, включающие использование аппаратных ключей и адаптивных систем.

**Ключевые слова:** контроль доступа; веб-безопасность; киберугрозы; многофакторная аутентификация; OAuth 2.0; тенденции развития.

### MODERN DEVELOPMENT VECTORS OF ACCESS CONTROL SYSTEMS IN WEB APPLICATIONS

Rogatykh Ksenia

The Bonch-Bruevich Saint Petersburg State University of Telecommunications  
22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mail: kseniarogatyh@yandex.ru

**Abstract.** The theses examine the evolution and key directions for improving authentication and authorization mechanisms as the foundation of web application security. The transition from traditional methods to multifactor and biometric approaches, as well as to decentralized authorization models, is analyzed. Special attention is paid to the



comprehensive counteraction of modern cyber threats through the integration of technologies and protocols. Promising trends, including the use of hardware keys and adaptive systems, are identified.

**Keywords:** access control; web security; cyber threats; multifactor authentication; OAuth 2.0; development trends.

Цифровая трансформация обуславливает критическую важность надежного контроля доступа к веб-приложениям. Эволюция механизмов аутентификации и авторизации становится центральным элементом в архитектуре информационной безопасности, направленной на минимизацию рисков несанкционированного доступа и утечек данных.

Эволюция методов аутентификации. Исторически сложилось, что аутентификация по паролям являлась доминирующим методом, однако ее уязвимости к фишингу и brute-force атакам стимулировали развитие более надежных схем. Многофакторная аутентификация (MFA) кардинально повышает безопасность, комбинируя знания пользователя, его имущество и биометрические характеристики. Одновременно наблюдается рост популярности токен-ориентированных подходов (JWT, OAuth), которые минимизируют передачу учетных данных и обеспечивают масштабируемость в микросервисных архитектурах. Биометрическая аутентификация, несмотря на проблемы конфиденциальности и требования к аппаратному обеспечению, задает новый стандарт удобства и безопасности [1].

Тенденции в моделях авторизации. Анализ показывает сдвиг от жестких централизованных моделей, таких как мандатный контроль доступа (MAC), применяемый в системах с повышенными требованиями секретности, к более гибким и децентрализованным решениям. Ролевая модель (RBAC) остается востребованной в корпоративной среде благодаря простоте администрирования, в то время как модели на основе токенов становятся де-факто стандартом для распределенных систем и API. Дискреционная модель (DAC) сохраняет актуальность в средах, где приоритетом является гибкость управления правами самими владельцами данных [2].

Комплексный подход к безопасности. Современная практика свидетельствует о необходимости интеграции различных методов и протоколов. Протоколы OAuth 2.0 и OpenID Connect формируют каркас для безопасного делегирования прав и аутентификации между сервисами. Безопасность данных обеспечивается применением стойких алгоритмов хеширования (bcrypt, Argon2), обязательным использованием HTTPS и эффективным управлением жизненным циклом токенов. Мониторинг сессий и анализ поведенческих аномалий становятся критически важными для выявления и пресечения атак в реальном времени [3].

Противодействие угрозам. Актуальный ландшафт угроз включает фишинг, кражу токенов, MITM-атаки и внутренние угрозы. Эффективная стратегия защиты требует комбинации технических и организационных мер: внедрение MFA для противодействия фишингу, использование защищенных идентификаторов сессии и принципа минимальных привилегий для снижения ущерба от утечек, а также применение систем анализа поведения для обнаружения подозрительной активности [4].

Развитие систем контроля доступа движется в сторону создания адаптивных, многоуровневых и пользовательско-ориентированных решений. Ключевыми перспективными направлениями являются дальнейшая интеграция биометрии, широкое внедрение аппаратных ключей безопасности и развитие контекстно-зависимых систем авторизации, анализирующих поведение и риски в реальном времени. Успешная защита веб-приложений будет определяться способностью разработчиков и организаций гибко комбинировать существующие и emerging-технологии в рамках единой стратегии безопасности.

#### СПИСОК ЛИТЕРАТУРЫ

1. Системы и методы аутентификации / Anti-Malware [Электронный ресурс] URL: <https://clck.ru/3BhWfM> (дата обращения: 25.07.2025).
2. Штеренберг, С. И. Обеспечение безопасности на высокоуровневой среде Windows / С. И. Штеренберг, Г. С. Бударный, Р. Р. Ахметов // Региональная информатика (РИ-2022) : Юбилейная XVIII Санкт-Петербургская международная конференция. Материалы конференции, Санкт-Петербург, 26–28 октября 2022 года. СПб.: СПОИСУ, 2022. С. 585–586. EDN TNRZPK.
3. Старосельский А. К., Жиренкин А. В. Авторизация и обмен данными в веб-приложениях с использованием протокола OAuth 2.0 // Современные технологии. Системный анализ. Моделирование. 2021. № 2 (70). С. 132–138.
4. Социальная инженерия: её методы и способы защиты / Г. С. Бударный, А. А. Дюсметова, А. А. Казанцев, А. В. Красов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): Сборник научных статей. XII Международная научно-техническая и научно-методическая конференция. В 4 т., Санкт-Петербург, 28 февраля 01 марта 2023 года. Том 1. СПб.: СПбГУ телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2023. С. 200–204. EDN PWVWPZ.

УДК 004.056

#### МЕТОДИКА КОМПЛЕКСНОЙ ОЦЕНКИ УРОВНЯ ЗРЕЛОСТИ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

**Сахаров Дмитрий Владимирович, Бирих Эрнест Владимирович, Гаврилов Павел Русланович**  
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевиков пр., 22, Санкт-Петербург, 193232, Россия  
e-mails: sguard7@mail.ru, be1982@mail.ru, general2pavel@yandex.ru

**Аннотация.** В условиях повсеместной цифровизации и роста числа киберугроз обеспечение надлежащего уровня информационной безопасности (ИБ) становится критически важной задачей для любой организации, будь то коммерческая компания или орган государственной власти. Существующие стандарты и лучшие практики задают ориентиры, однако для эффективного управления и планомерного повышения защищенности необходим

инструмент оценки текущего состояния ИБ. В статье предлагается методика комплексной оценки уровня зрелости системы информационной безопасности, основанная на анализе ключевых доменов управления ИБ и позволяющая выявить слабые места и определить приоритетные направления для развития.

**Ключевые слова:** информационная безопасность; система менеджмента ИБ (СМИБ); оценка зрелости; модель зрелости; управление рисками; киберугрозы; ГОСТ Р ИСО/МЭК 27001; NIST SP 800-53; ФЗ-152.

## A METHOD FOR COMPREHENSIVE ASSESSMENT OF THE LEVEL OF MATURITY OF AN ORGANIZATION'S INFORMATION SECURITY SYSTEM

Sakharov Dmitry, Birikh Ernest, Gavrilo Pavel

St. Petersburg State University of Telecommunications. Prof. M. A. Bonch-Brujevich

22 Bolshhevikov Av, St. Petersburg, 193232, Russia

e-mails: sguard7@mail.ru, be1982@mail.ru, general2pavel@yandex.ru

**Abstract.** In the context of ubiquitous digitalization and the growing number of cyber threats, ensuring an adequate level of information security (IS) becomes a critical task for any organization, whether it is a commercial company or a government body. Existing standards and best practices provide guidelines, but an effective management and systematic improvement of security require a tool to assess the current state of IS. This article proposes a methodology for a comprehensive assessment of the information security system maturity level, based on the analysis of key IS management domains, allowing to identify weaknesses and determine priority areas for development.

**Keywords:** Information Security; ISMS, Maturity Assessment; Maturity Model; Risk Management; Cyber Threats; GOST R ISO/IEC 27001; NIST SP 800-53; Federal Law 152-FZ.

В современном мире организации сталкиваются с постоянно эволюционирующим ландшафтом киберугроз [1]. Успешная реализация этих угроз может привести к финансовым, операционным и репутационным потерям. Важным аспектом является также соблюдение законодательных и регуляторных требований, таких как Федеральный закон «О персональных данных» [2], и специфических отраслевых стандартов, например, ГОСТ Р 57580.1 для финансовых организаций [3].

Для построения эффективной защиты многие организации внедряют системы менеджмента информационной безопасности (СМИБ). Основой для таких систем часто служат признанные стандарты, в частности, российский ГОСТ Р ИСО/МЭК 27001-2021 [4], определяющий требования к СМИБ. Детализированные перечни мер и контролей безопасности могут быть взяты из таких источников, как NIST SP 800-53 [5] или приложения к самому ГОСТ Р ИСО/МЭК 27001.

Однако наличие формально описанных процессов и внедренных средств защиты не всегда означает их реальную эффективность. Необходимо оценивать, насколько хорошо эти процессы выполняются, управляются и совершенствуются — то есть их уровень зрелости. Для этой цели применяются модели зрелости, позволяющие структурированно оценить развитие процессов ИБ в организации по определенной шкале [6]. Как показано в обзоре [6], существуют различные модели зрелости (например, CMMI, COBIT PAM, на основе ISO/IEC стандартов), но часто требуется их адаптация под конкретные задачи и стандарты организации.

Предлагаемая методика комплексной оценки уровня зрелости СМИБ базируется на следующих принципах:

1. Оценка охватывает ключевые области управления ИБ, соответствующие структуре стандартов и общим практикам [7] (например, Политика ИБ, Управление активами, Контроль доступа, Криптография, Физическая безопасность, Безопасность операций, Безопасность коммуникаций, Управление инцидентами ИБ, Обеспечение непрерывности и др.).

2. Применение шкалы зрелости (например, 5-уровневой, как обсуждается в обзорах моделей зрелости) для оценки каждого процесса/домена.

3. Использование четких критериев для каждого уровня зрелости, основанных на требованиях стандартов и лучших практиках [7].

Процесс оценки включает:

- определение области оценки (вся организация или отдельные подразделения/системы);
- анализ документации СМИБ, интервью, аудит конфигураций и процессов;
- оценка уровня зрелости по каждому процессу/домену на основе собранных данных и критериев;
- расчет общего или доменных показателей зрелости;
- визуализация и формирование отчета с анализом пробелов и рекомендациями.

Применение данной методики позволяет не только оценить текущее состояние СМИБ в соответствии с требованиями, но и, что важнее, выявить слабые звенья и определить приоритеты для дальнейшего развития и *повышения* общего уровня защищенности организации [8]. Результаты оценки служат основой для разработки дорожной карты совершенствования СМИБ, обоснования необходимых ресурсов и демонстрации прогресса руководству и регуляторам.

## СПИСОК ЛИТЕРАТУРЫ

1. Отчет о глобальных рисках 2024 (The Global Risks Report 2024) // World Economic Forum. [Электронный ресурс]. URL: <https://www.weforum.org/publications/global-risks-report-2024/>.
2. Федеральный закон О персональных данных от 27.07.2006 N 152-ФЗ (ред. от 06.02.2023). // Собрание законодательства РФ. 31.07.2006. № 31 (1 ч.). ст. 3451.

3. ГОСТ Р 57580.1-2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер. М.: Стандартинформ, 2017.
4. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. М.: Стандартинформ, 2021.
5. NIST Special Publication 800-53 Revision 5. Security and Privacy Controls for Information Systems and Organizations. // National Institute of Standards and Technology. September 2020. [Электронный ресурс]. URL: <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>.
6. Милославская Н.Г., Сагиров Р.А. Обзор моделей зрелости процессов управления информационной безопасностью // Экономика и качество систем связи. 2018. № 4 (10). С. 11-21.
7. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие. 4-е изд., перераб. и доп. М.: ИД «ФОРУМ»: ИНФРА-М, 2023. 416 с. ISBN 978-5-8199-0988-0, 978-5-16-017955-8.
8. Гафнер В. В. Информационная безопасность: Учебное пособие. Ростов-на-Дону: Феникс, 2010. 324 с. ISBN 978-5-222-16808-7.

УДК 004.056

## СРАВНИТЕЛЬНОЕ ИССЛЕДОВАНИЕ СТЕПЕНИ СОХРАННОСТИ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ В БАЙТ-КОДАХ ЯЗЫКОВ ПРОГРАММИРОВАНИЯ, КОМПИЛИРУЕМЫХ ДЛЯ ВИРТУАЛЬНОЙ МАШИНЫ JAVA

Соколов Игорь Всеволодович

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевикова пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mail: isokol0303@gmail.com

**Аннотация.** Проблема защиты авторского права с каждым днём становится всё более серьёзной проблемой для компаний, занимающихся разработкой программного обеспечения. В данном исследовании рассматривается устойчивость байт-кода к вложению цифрового водяного знака в различных языках программирования на платформе JVM с последующим сравнительным анализом.

**Ключевые слова:** цифровой водяной знак; байт-код; Scala; Java; Kotlin; статический анализ.

## COMPARATIVE STUDY OF DIGITAL WATERMARK PERSISTENCE IN BYTECODE OF PROGRAMMING LANGUAGES COMPILED FOR JAVA VIRTUAL MACHINE

Sokolov Igor

The Bonch-Bruevich Saint Petersburg State University of Telecommunications  
22 Bolshhevikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mail: isokol0303@gmail.com

**Abstract.** The issue of copyright protection is becoming an increasingly serious problem for software development companies every day. This study examines the stability of bytecode to embedding a digital watermark in various programming languages on the JVM platform, followed by a comparative analysis.

**Keywords:** digital watermark; bytecode; Scala; Java; Kotlin; static analysis.

В статье проводится сравнительный анализ устойчивости байт-кода различных языков программирования на платформе JVM (Java, Kotlin, Scala) для вложения цифрового водяного знака.

Исследование выявляет, что сложность и структура генерируемого байт-кода напрямую влияют на возможности скрытного и устойчивого внедрения защитных меток. Scala демонстрирует наилучшие результаты благодаря сложным многоуровневым структурам, *implicit*-логике и функциональным конструкциям, обеспечивающим до 12 точек вложения с высокой скрытностью. Kotlin занимает промежуточное положение, используя метаданные, лямбда-выражения и *inline*-функции для создания 8 точек вложения. Java показывает наименьшую эффективность с 5 точками вложения и средней скрытностью из-за простого и предсказуемого байт-кода [1–3].

Эксперименты подтвердили, что увеличение размера файлов и времени выполнения незначительно, а корректность работы программ сохраняется на 100% во всех случаях. Результаты исследования позволяют рекомендовать Scala и Kotlin как предпочтительные языки для разработки приложений, требующих защиты авторских прав на уровне байт-кода [4–6].

Несмотря на увеличение размера *class*-файлов до 1.8, общая корректность и стабильность исполнения программы остаются без изменений [7, 8]. Kotlin занимает промежуточную позицию: наличие лямбда-выражений, контрактов и *inline*-функций расширяет количество безопасных точек вставки. Java же, предоставляет ограниченные возможности для скрытного вложения, и цифровой водяной знак при дизассемблировании может быть идентифицирован относительно легко [9, 10].

Таким образом, языки Scala и Kotlin можно рассматривать как более защищённую среду для разработки программного обеспечения с механизмами защиты авторства на уровне байт-кода, благодаря наличию глубокой структуры, повышающей устойчивость к анализу и модификации [11, 12].

Проведённое исследование продемонстрировало, что устойчивость байт-кода программ к вложению цифрового водяного знака существенно зависит от особенностей исходного языка программирования и

характеристик генерации промежуточного представления. Язык Scala, благодаря своей высокоуровневой семантике, implicit-структурам и разветвлённой модели потока исполнения, предоставляет наиболее удобные условия для скрытого и устойчивого вложения ЦВЗ.

Kotlin показывает хорошие результаты за счёт дополнительной метainформации и наличия встроенных функциональных конструкций. Java, хотя и обладает простым и предсказуемым байт-кодом, наименее устойчива к вложению с точки зрения маскировки и числа безопасных точек [13, 14].

#### СПИСОК ЛИТЕРАТУРЫ

1. Gulzar, I. Methodology for Embedding a Digital Watermark in Java Application Class Files Resistant to Decompilation Attacks Aimed at Its Destruction. 2024.
2. Barthe, G., Burdy, L., Requet, A., & Rusu, V. Reasoning About Exceptional Behavior At the Level of Java Bytecode. In Formal Methods for Open Object-Based Distributed Systems. Springer. 2005.
3. Collberg, C., Thomborson, C., & Low, D. Dynamic Path-Based Software Watermarking. University of Arizona. 2004.
4. Шариков П.И., Красов А.В., Штеренберг С.И. Методика создания и вложения цифрового водяного знака в исполняемые java файлы на основе замен опкодов // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. №3. С. 66-70.
5. Шариков, П. И. Методика создания и скрытого вложения цифрового водяного знака в байт-код class-файла на основе не декларированных возможностей виртуальной машины java / П. И. Шариков // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2023. № 7-2. С. 165-174. DOI 10.37882/2223-2982.2023.7-2.37. EDN YBEWYQ.
6. Дудников, И. А. Методика анализа журналов событий информационных систем с использованием Elasticsearch для обнаружения сигналов о вредоносных действиях в информационной системе / И. А. Дудников, П. И. Шариков, А. В. Майоров // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2025. № 1. С. 120-134. DOI 10.61260/2218-130X-2025-1-120-134. EDN ZQCEXG.
7. Свидетельство о государственной регистрации программы для ЭВМ № 2015611539 Российская Федерация. RPA (rationabile progressio aggredi) (лат.) : № 2014662384 : заявл. 02.12.2014 : опубл. 30.01.2015 / С. И. Штеренберг, В. И. Андрианов, В. А. Липатников, С. В. Костарев ; заявитель СПбГУ телекоммуникаций им. проф. М.А.Бонч-Бруевича. EDN KMMBIK.
8. Штеренберг, С. И. Исследование методики адаптивных атак на основе скрытого вложения в исполнимые файлы / С. И. Штеренберг, В. И. Андрианов // Наука, Техника, Инновации 2014 : сборник статей Международной научно-технической конференции, Брянск, 25–27 марта 2014 года / Под общей редакцией А.Л. Сафонова. Брянск: Общество с ограниченной ответственностью «Надежные машины», 2014. С. 287-294. EDN SWRRUF.
9. Методика скрытного внедрения исполняемого кода в распределенные информационные системы с помощью агентного подхода / С. И. Штеренберг, В. В. Нефедов, В. И. Андрианов, В. А. Липатников // Вестник СПбГУПТД. Серия 1: Естественные и технические науки. 2023. № 1. С. 76-85. DOI 10.46418/2079-8199\_2023\_1\_13. EDN PRJWBG.
10. Аксенов, К. Д. Защита медицинских данных в эпоху развития технологий искусственного интеллекта / К. Д. Аксенов, А. В. Красов // Региональная информатика (РИ-2024) : Материалы XIX Санкт-Петербургской международной конференции, Санкт-Петербург, 23–25 октября 2024 года. СПб.: СПОИСУ, 2024. С. 89-90. EDN ASDYIF.
11. Беккель, Л. С. Применение сетевой стеганографии в UDP-потоках для обеспечения безопасной передачи данных / Л. С. Беккель, А. В. Красов, Е. Ю. Герлинг // Вестник СПбГУПТД. Серия 1: Естественные и технические науки. 2025. № 1. С. 63-67. DOI 10.46418/2079-8199\_2025\_1\_12. EDN GAGFDM.
12. Свидетельство о государственной регистрации программы для ЭВМ № 2024691520 Российская Федерация. Программное обеспечение автоматизированного сбора и структурирования журналов приложений для выявления аномалий в информационных системах : заявл. 10.12.2024 : опубл. 23.12.2024 / А. В. Майоров, П. И. Шариков, А. В. Красов, А. И. Пешков ; заявитель Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича. EDN IURLQM.
13. Штеренберг, С. И. Обеспечение безопасности на высокоуровневой среде Windows / С. И. Штеренберг, Г. С. Бударный, Р. Р. Ахметов // Региональная информатика (РИ-2022) : Юбилейная XVIII Санкт-Петербургская международная конференция. Материалы конференции, Санкт-Петербург, 26–28 октября 2022 года. СПб.: СПОИСУ, 2022. С. 585-586. EDN TNRZPK.
14. Волостных, В. А. Проблемы обеспечения безопасности персональных данных в высших учебных заведениях / В. А. Волостных, С. И. Штеренберг, Ю. В. Гвоздев // Информационные технологии и телекоммуникации. 2014. Т. 2, № 4. С. 134-141. EDN TKSXTZ.

УДК 004.75-004.054

#### **КОМПРОМИССЫ И РИСКИ ПРИ ВНЕДРЕНИИ РАСПРЕДЕЛЁННЫХ ХРАНИЛИЩ В ЗАЩИЩЁННЫХ ВИРТУАЛИЗИРОВАННЫХ СРЕДАХ: ОПЫТ ИСПОЛЬЗОВАНИЯ СЕРН В ПК СВ «БРЕСТ»**

**Строило Анна Юрьевна, Цветков Александр Юрьевич**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mails: stroilana@yandex.ru, aleksandr.tcvetkov@sut.ru

**Аннотация.** Выбор распределённого хранилища для защищённой виртуализированной среды требует комплексной оценки технических, инфраструктурных и организационных ограничений. Серн, несмотря на декларируемую отказоустойчивость и масштабируемость, предъявляет высокие требования к сети, вычислительным ресурсам и квалификации персонала, что критично в регулируемых и ресурсоограниченных средах. В таких условиях локальные решения вроде LVM могут оказаться предпочтительнее благодаря простоте, предсказуемости и лучшей совместимости с требованиями информационной безопасности.

**Ключевые слова:** распределенная система хранения данных; ПК СВ «Брест»; защищённая виртуализированная среда; выбор системы хранения.

## TRADE-OFFS AND RISKS WHEN IMPLEMENTING DISTRIBUTED STORAGE IN SECURE VIRTUALIZED ENVIRONMENTS: THE EXPERIENCE OF USING CEPH IN THE SOFTWARE COMPLEX OF VIRTUALIZATION TOOLS «BREST»

**Stroilo Anna, Tsvetkov Alexandr**

The Bonch-Bruевич Saint Petersburg State University of Telecommunications  
22 Bolshhevikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mails: stroiloana@yandex.ru, aleksandr.tsvetkov@sut.ru

**Abstract.** Choosing distributed storage for a secure virtualized environment requires a comprehensive assessment of technical, infrastructural, and organizational constraints. Despite its declared fault tolerance and scalability, Ceph places high demands on the network, computing resources, and staff qualifications, which is critical in regulated and resource-constrained environments. In such circumstances, local solutions like LVM may be preferable due to simplicity, predictability, and better compatibility with information security requirements.

**Keywords:** distributed data storage system; software complex of virtualization tools «Brest»; secure virtualized environment; choice of storage system.

Выбор распределённой системы хранения данных для защищённой виртуализированной среды — это не просто техническое решение, а стратегическое решение, от которого зависит не только производительность, но и устойчивость всей ИТ-инфраструктуры в долгосрочной перспективе [1].

Особое значение приобретает этот вопрос при использовании отечественных платформ, таких как Программный комплекс «Средства виртуализации «Брест», где требования к безопасности, надёжности и предсказуемости работы выходят на первый план. Распространённое убеждение, что современные распределённые хранилища вроде Ceph автоматически обеспечивают высокую производительность и отказоустойчивость, требует серьёзной корректировки — на практике их внедрение сопряжено со скрытыми издержками, которые могут свести на нет ожидаемые преимущества [2].

Результаты практического применения Ceph в составе ПК СВ «Брест» показывают, что за впечатляющими цифрами IOPS и масштабируемостью стоят реальные ограничения, которые проявляются именно в условиях эксплуатации.

Высокая производительность при случайном доступе к данным достигается ценой значительной нагрузки на центральный процессор - в отдельных сценариях загрузка центрального процессора (ЦП) превышала 30%, что в восемнадцать раз выше, чем при использовании локального хранилища LVM.

Для ресурсоограниченных сред, характерных для многих государственных и корпоративных инфраструктур, такой рост вычислительной нагрузки может стать критичным, вынуждая либо увеличивать аппаратные ресурсы, либо жертвовать производительностью других сервисов.

Не менее важным фактором оказывается сетевая инфраструктура. Средние задержки в 450 миллисекунд, а в пиковых ситуациях — до 10 секунд, делают Ceph малоприспособленным для задач, чувствительных ко времени отклика, если сеть не оптимизирована под требования распределённого хранилища. Это означает, что переход на Ceph — это не просто замена дискового массива, а модернизация всей сетевой архитектуры, что влечёт за собой дополнительные затраты и сложности при проектировании.

Кроме технических ограничений, нельзя игнорировать и человеческий фактор. Эксплуатация кластера Ceph требует от администраторов глубоких знаний в области распределённых систем, умения настраивать репликацию, балансировать нагрузку и оперативно реагировать на сбои [3].

В условиях дефицита квалифицированных кадров это может привести к увеличению времени простоя и снижению общей надёжности системы.

В то же время локальное хранилище LVM, несмотря на скромные показатели при работе с мелкими файлами, остаётся предпочтительным выбором там, где важны простота управления, минимальная задержка и предсказуемое поведение — например, при развёртывании виртуальных машин или резервном копировании больших массивов данных.

Особую актуальность приобретает вопрос информационной безопасности. Функции самовосстановления и репликации, делающие Ceph устойчивым к сбоям, одновременно усложняют процессы аудита и контроля целостности данных.

В защищённых средах, где каждое действие должно быть прослеживаемо и верифицируемо, это создаёт дополнительные риски, требующие внедрения сложных систем мониторинга и логирования.

Таким образом, внедрение распределённого хранилища — это не технологическое улучшение «по умолчанию», а осознанный выбор, требующий взвешенного анализа не только технических характеристик, но и организационных, экономических и кадровых возможностей.

Только такой комплексный подход позволяет избежать типичных ошибок и обеспечить стабильную, безопасную и эффективную работу виртуализированной инфраструктуры в долгосрочной перспективе.

### СПИСОК ЛИТЕРАТУРЫ

1. Мазур Э. М. Распределённые системы хранения данных: анализ, классификация и выбор // Перспективы развития информационных технологий. 2015. № 26. С. 33-60. EDN UZQENL.
2. Таненбаум Э. Распределённые системы. Принципы и парадигмы. Санкт-Петербург: Питер, 2003. 912 с. ISBN 5-272-00053-6.
3. Руководство пользователя программного комплекса «Средство виртуализации „Брест“» [Электронный ресурс]. АО «РусБИТех», 2023. 94 с. URL: <https://astra.ru/upload/iblock/ca7/ksb19b99tevlkediig2iwi6zx4pbbs16.pdf>

УДК 004.056

## УГРОЗЫ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ АГЕНТОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

**Трофимов Евгений Александрович<sup>1</sup>, Виткова Лидия Андреевна<sup>1,2</sup>**

<sup>1</sup> Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича  
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

<sup>2</sup> СПб ФИЦ РАН

14-я линия ВО, 39, Санкт-Петербург, 199178, Россия

e-mails: diad.hedi@gmail.com, vitkova.la@sut.ru

**Аннотация.** В работе рассматриваются специфические угрозы безопасности, возникающие при использовании агентов ИИ (искусственного интеллекта) в корпоративной цифровой среде. В отличие от традиционных моделей, такие агенты способны к автономному принятию решений, долговременному хранению контекста и выполнению действий в разнородных инфраструктурах. Проведен анализ возможных векторов атак, включая подмену логики планирования, манипуляции памятью и инструментами, а также сложности обеспечения идентификации и управления полномочиями. Предложены общие принципы проектирования безопасных систем с элементами автономии.

**Ключевые слова:** агенты ИИ; безопасность технологий ИИ; конструктивная информационная безопасность; верификация данных.

## SECURITY THREATS IN ADAPTIVE ARTIFICIAL INTELLIGENCE AGENTS

**Trofimov Evgeniy<sup>1</sup>, Vitkova Lidiya<sup>1,2</sup>**

<sup>1</sup> The Bonch-Bruevich Saint Petersburg State University of Telecommunications  
22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia

<sup>2</sup> St. Petersburg Federal Research Center of the Russian Academy of Sciences  
39 14th Line VO, St. Petersburg, 199178, Russia  
e-mails: diad.hedi@gmail.com, vitkova.la@sut.ru

**Abstract.** This article examines specific security threats arising from the use of artificial intelligence (AI) agents in enterprise digital environments. Unlike conventional models, such agents can make autonomous decisions, retain long-term context, and execute actions across heterogeneous infrastructures. We analyze key attack vectors, including manipulation of planning logic, tampering with memory, and the misuse of integrated tools, as well as challenges in identity and access management and privilege control. The article proposes general design principles for building secure systems that incorporate autonomous capabilities.

**Keywords:** AI agents; AI security; secure by design; data verification.

Современные агенты ИИ, используемые в корпоративных информационных системах, характеризуются высокой степенью автономности. Воспринимая окружение и поддерживая внутреннее состояние и контекст, такие компоненты самостоятельно принимают решения и выполняют операции через подключённые инструменты без участия администратора.

Такие свойства расширяют возможные сценарии применения, но при этом создают дополнительные риски. Увеличивается вероятность несанкционированного воздействия на поведение агента, а существующие меры безопасности не всегда позволяют эффективно контролировать его действия. Это вызывает необходимость пересмотра подходов к обеспечению безопасности в цифровой инфраструктуре, где задействованы автономные программные компоненты.

Одной из основных угроз является вмешательство в процесс планирования, на основе которого агент выбирает действия [1]. Планирование представляет собой внутреннюю логику, с помощью которой агент оценивает доступные варианты и решает, что делать в конкретной ситуации. Если на этот механизм удастся повлиять, например через изменение приоритетов целей или подмену условий выбора, поведение агента может отклониться от ожидаемого. Агент может продолжать выполнять действия, которые внешне кажутся допустимыми, но фактически противоречат целям пользователя или организации. Такая угроза проявляется не сразу и часто остается незамеченной, поскольку подобные отклонения происходят в пределах формально допустимого поведения.

Следующий риск связан с долговременной памятью и контекстом агента, которые фиксируют сведения о прошлых действиях и событиях для последующих решений. Такая память формирует профиль поведения и влияет на будущую стратегию. Если нарушитель получает доступ к таким данным и вносит изменения, агент начинает опираться на ложные или искажённые сведения. Возникают устойчивые отклонения, которые выглядят логично, но не соответствуют реальной обстановке. Также возможен накопительный эффект, при котором каждое новое искажение усиливает предыдущее и приводит к постепенному уходу от исходных целей. Диагностика причин нарушений в таких условиях затруднена.

Отдельная уязвимость связана с инструментами агента, под которыми понимаются вызовы API (программного интерфейса приложения), операции с базами данных, запуск скриптов, обращения к очередям задач, облачным сервисам и системам управления. Эти интерфейсы выполняют операции с побочными

эффектами и используют доверенные учетные данные агента. Злоумышленник может не взламывать сам агент, а подталкивать его к выполнению нужного вызова через подмену контекста или задания.

Риск возрастает, когда у агента широкие привилегии, отсутствует жесткий перечень разрешенных операций, не проверяются схемы и допустимые значения параметров, не разделены идентичности пользователя и агента и нет отдельного журнала их действий. Типовые сценарии включают чтение или выгрузку таблиц с избыточным набором полей, выполнение скрипта в производственной среде, изменение конфигурации через административный API и пересылку полученных секретов во внешний канал.

Часто используется цепочка из нескольких на вид безобидных шагов, которая в сумме приводит к утечке или изменению данных. Отсутствие подтверждений для чувствительных операций и предварительной проверки предполагаемых действий делает такие атаки почти неотличимыми от штатной работы [2].

Опасность представляет и нечеткое распределение полномочий. Часто в системах отсутствует четкое разделение между действиями пользователя и действиями агента. Это затрудняет аудит, усложняет расследование инцидентов и делает невозможным эффективное управление доступом. Если в системе присутствует несколько агентов, возникают дополнительные риски.

Агенты могут обмениваться данными, перенимать поведенческие модели, делиться результатами наблюдений. При недостаточной изоляции ошибка или вмешательство в одного из них может повлиять на поведение остальных. В условиях, когда агенты работают в общей среде и имеют возможность сохранять и передавать информацию, это становится критичным.

Для снижения этих рисков необходимо учитывать особенности на стадии проектирования. Полезным оказывается введение изоляции, а также других базовых принципов безопасного проектирования (secure by design), таких как ограничение привилегий, поведенческий контроль и защита каналов взаимодействия [3]. Агент должен принимать данные только из проверенных источников и через защищенные каналы с проверкой формата и происхождения.

Права задают по принципу минимально необходимых, перечень доступных инструментов ограничивают, а каждое обращение проверяют на допустимость и параметры. Поведенческий анализ сопоставляет текущую активность с эталонной моделью и выявляет отклонения. Журналы ведут полно и неизменяемо с указанием инициатора, использованного инструмента, переданных параметров и результата, что обеспечивает прозрачность и ускоряет восстановление после инцидента.

Таким образом, агенты ИИ, обладающие автономией и способностью к накоплению поведенческого опыта, предъявляют новые требования к обеспечению безопасности в корпоративной цифровой инфраструктуре. Их поведение не всегда поддается прямому контролю, а действия могут быть формально допустимыми, но при этом не соответствовать интересам пользователя или организации. Это требует пересмотра существующих подходов к защите систем и построения архитектур, в которых риски учитываются на этапе проектирования.

#### СПИСОК ЛИТЕРАТУРЫ

1. Deng Z., Guo Y., Han C., Ma W., Xiong S. Wen S., Xiang Y. AI Agents Under Threat: A Survey of Key Security Challenges and Future Pathways [Электронный ресурс] // URL: <https://arxiv.org/abs/2406.02630> (дата обращения: 28.07.2025).
2. Wang Y., Pan Y., Guo S., Su Z. Security of Internet of Agents: Attacks and Countermeasures [Электронный ресурс] // URL: <https://arxiv.org/abs/2505.08807> (дата обращения: 31.07.2025).
3. Narajala V. S., Narayan O. Securing Agentic AI: A Comprehensive Threat Model and Mitigation Framework for Generative AI Agents [Электронный ресурс] // URL: <https://arxiv.org/abs/2504.19956> (дата обращения: 01.08.2025).

УДК 004.056.53

#### НОВЫЕ СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ И ДАННЫХ В СФЕРЕ УСЛУГ ТЕЛЕПРИСУТСТВИЯ

**Ушаков Игорь Александрович, Штеренберг Станислав Игоревич, Панков Арсений Владимирович**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

Большевикова пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

e-mails: ushakov.ia@sut.ru, shterenberg.si@sut.ru, pankov.av@sut.ru

**Аннотация.** Сбор данных представляет собой фундаментальный этап в процессе построения систем на основе искусственного интеллекта (ИИ) в сфере услуг телеприсутствия. Этот этап включает в себя систематическое извлечение информации о сетевом трафике, системных журналах, событиях безопасности и других источниках, которые могут содержать индикаторы компрометации и признаки атак. Данные могут быть получены как из реальных сетевых сред, так и из симулированных или тестовых сетей, что позволяет учитывать разнообразные сценарии и типы атак. Важным аспектом является обеспечение репрезентативности и разнообразия данных, чтобы модели ИИ могли эффективно обобщать и распознавать различные шаблоны атак. Это требует тщательной аннотации и маркировки данных, чтобы алгоритмы могли различать легитимную активность от подозрительной.

**Ключевые слова:** услуги телеприсутствия; интеллектуальные системы; защита информации; размерность данных; сетевые атаки.

## NEW WAYS TO PROTECT INFORMATION AND DATA IN THE FIELD OF TELEPRESENCE SERVICES

Ushakov Igor, Shterenberg Stanislav, Pankov Arseniy

The Bonch-Bruевич Saint Petersburg State University of Telecommunications

22 Bolshhevikov Av, bldg 1, St. Petersburg, 193232, Russia

e-mails: ushakov.ia@sut.ru, shterenberg.si@sut.ru, pankov.av@sut.ru

**Abstract.** Data collection is a fundamental step in the process of building systems based on artificial intelligence (AI) in the field of telepresence services. This stage includes the systematic extraction of information about network traffic, system logs, security events, and other sources that may contain indicators of compromise and signs of attacks. Data can be obtained from real network environments, as well as from simulated or test networks, which allows you to consider a variety of scenarios and types of attacks. An important aspect is to ensure the representativeness and diversity of data so that AI models can effectively summarize and recognize various attack patterns. This requires careful Abstract and labeling of the data so that algorithms can distinguish legitimate activity from suspicious activity.

**Keywords:** telepresence services; intelligent systems; information security; network attacks; data dimension.

Оптимизация данных направлена на повышение их качества и устранение избыточности. Этот процесс включает в себя очистку данных от шумов, устранение дубликатов, заполнение пропусков, а также применение методов отбора признаков и уменьшения размерности данных [1]. Например, для отбора признаков можно использовать такие методы, как анализ главных компонент (PCA) или регуляризация Lasso, которые помогают выявить наиболее информативные характеристики и сократить объем данных, не теряя при этом значимой информации. Оптимизация позволяет улучшить производительность алгоритмов ИИ, сократить время их обучения и повысить точность детекции атак [2]. В частности, уменьшение размерности данных может значительно снизить вычислительные затраты и ускорить процесс обработки. В данном докладе будет представлен обзор новой модели, используемой для эффективного сбора данных, необходимых для построения систем обнаружения сетевых атак на основе ИИ. Будут рассмотрены преимущества и недостатки различных подходов [3].

В новой модели представлена практическая часть внедрения и эксплуатации многоагентной IDS в реальной корпоративной сети [4]. Каждый из восьми последовательно описанных этапов — от момента зеркалирования «живого» трафика до автоматического реагирования и самоадаптации моделей — отвечает за конкретную техническую функцию в сквозном процессе обнаружения атак [5]. Вместе они формируют воспроизводимый рабочий цикл, позволяющий системе одновременно сохранять низкую задержку, высокую точность и устойчивость к дрейфу статистики и переобучению [6].

В итоге первым крупным результатом исследования стало формирование универсального цикла подготовки и балансировки данных. Дополнительная генерация редких атак через вариационный GAN привела к естественной балансировке позитивного класса без искусственного реплика-оверсэмплинга; именно такое сочетание позволило удержать долю позитивов в районе двадцати процентов батча, что эмпирически оказалось оптимальным между чувствительностью и устойчивостью к ложным срабатываниям [7].

Вторым достижением стало введение унифицированной стратегии обучения для архитектур, радикально различающихся по внутренней механике: сверточных, рекуррентных, полносвязных и гибридных ветвей. За счёт единого расписания скорости обучения, идентичного набора регуляризаторов (dropout, L2-штраф, adversarial mini-batches) и кросс-архитектурной функции потерь с фокус-термом (focal-modifier) все подмодели демонстрируют схожую динамику сходимости и синхронно достигают плато качества. Это обстоятельство существенно упростило дальнейший этап ансамблирования: метаклассификатору не пришлось «ретранслировать» выходы с разной шкалой уверенности; напротив, температурная калибровка показала минимальное расхождение по зет-скор-диапазону [8].

Особое место в докладе занимает контур самозащиты от переобучения нейросети работающей с программами для задач услуг в сфере телеприсутствия [9]. В цельном виде он представляет собой первое в отечественной литературе решение, которое опирается не на эвристическую проверку контрольной выборки, а на динамический анализ «поведенческих» телеметрических метапризнаков самой модели [10]. Результаты испытаний подтвердили, что такой подход способен обнаруживать начало деградации за 4-6 часов до того, как понизится сводная AUC. Более того, при появлении искусственного дрейфа (переход большей части пользователей на HTTP/2 и резкий рост MTU-пакетов) контур зафиксировал аномалию через 27 минут после начала изменения и автоматически инициировал fine-tune только LSTM-ветви, не трогая остальные агенты; время полной стабилизации — 28 мин, снижение ложноположительных до 0,86 % — показатели, которые ранее достигались исключительно за счёт ручного вмешательства аналитиков SOC.

*Исследование выполнено при финансовой поддержке Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, соглашение № 071-03-2025-005, «Прикладные научные исследования в области создания сервисов и приложений в перспективных сетях связи» (регистрационный номер ПТНИ: 1024032900317-4).*

## СПИСОК ЛИТЕРАТУРЫ

1. Волков, А. Н. Туманные вычисления в сетях IMT-2030 для услуг телеприсутствия / А. Н. Волков, А. Е. Кучерявый // XIV Всероссийское совещание по проблемам управления : сборник научных трудов, Москва, 17–20 июня 2024 года. Москва: Институт проблем управления им. В.А. Трапезникова РАН, 2024. С. 2295-2297. EDN JXYICQ.



2. Модельная сеть для исследований и обучения в области услуг телеприсутствия / А. Е. Кучерявый, М. А. Маколкина, А. И. Парамонов [и др.] // Электросвязь. 2022. № 1. С. 14-20. DOI 10.34832/ELSV.2022.26.1.001. EDN GBQWCV.
3. Optimized Data Transmission and Signal Processing for Telepresence Suits in Multiverse Interactions / A. Volkov, A. Muthanna, A. Paramonov [et al.] // Journal of Sensor and Actuator Networks. 2024. Vol. 13, No. 6. P. 82. DOI 10.3390/jsan13060082. EDN VBEMLB.
4. Ali, R. A. Artificial intelligence driven 5G and beyond networks / R. A. Ali, A. Koucheryavy // Telecom IT. 2022. Vol. 10, No. 2. P. 1-13. DOI 10.31854/2307-1303-2022-10-2-1-13. EDN VAFXSU.
5. Тамбовский, А. Н. Архитектура сервиса сбора данных для обнаружения инсайдерских угроз в файловых системах Linux / А. Н. Тамбовский, И. А. Ушаков // Подготовка профессиональных кадров в магистратуре в эпоху цифровой трансформации (ПКМ-2024) : Сборник лучших докладов V Всероссийской научно-технической и научно-методической конференции магистрантов и их руководителей. В 2-х томах, Санкт-Петербург, 03–05 декабря 2024 года. СПб.: СПбГУ телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2025. С. 273-276. EDN AZDKWU.
6. Проничев, В. Д. Автоматизированный анализ изменений в сетевых конфигурациях устройств на основе нейронных сетей / В. Д. Проничев, И. А. Ушаков // Подготовка профессиональных кадров в магистратуре в эпоху цифровой трансформации (ПКМ-2024) : Сборник лучших докладов V Всероссийской научно-технической и научно-методической конференции магистрантов и их руководителей. В 2-х томах, Санкт-Петербург, 03–05 декабря 2024 года. СПб.: СПбГУ телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2025. С. 443-448. EDN DDZZOT.
7. Ушаков, И. А. Анализ методов обеспечения безопасности в сетях LTE / И. А. Ушаков, А. И. Черкашин // 65-я научно-техническая конференция профессорско-преподавательского состава, научных работников и аспирантов (НТК ППС 2025) : Сборник научных статей. В 3 т., Санкт-Петербург, 17–21 февраля 2025 года. СПб.: СПбГУ телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2025. С. 506-511. EDN IRLJHD.
8. Разработка блока обнаружения и коррекции ошибок для устройства диагностирования каналов передачи цифровой информации / А. К. Сагдеев, И. Г. Штеренберг, С. И. Штеренберг, О. М. Виноградова // Вестник СПбГУПТД. Серия 1: Естественные и технические науки. 2020. № 1. С. 15-24. DOI 10.46418/2079-8199\_2020\_1\_3. EDN PYQLFU.
9. Разработка методов обеспечения безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения / С. И. Штеренберг, А. И. Москальчук, В. А. Коптелова, О. М. Виноградова // Вестник СПбГУПТД. Серия 1: Естественные и технические науки. 2021. № 1. С. 32-38. DOI 10.46418/2079-8199\_2021\_1\_5. EDN VUPDRU.
10. Штеренберг, С. И. Обнаружение вторжений в распределенных информационных системах на основе методов скрытого мониторинга и анализа больших данных : специальность 05.13.19 «Методы и системы защиты информации, информационная безопасность» : диссертация на соискание ученой степени кандидата технических наук / Штеренберг Станислав Игоревич, 2018. 182 с. EDN NLQRSK.

УДК 004.032.26

## АНАЛИЗ ВИДОВ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ОБНАРУЖЕНИЯ АТАК НА ОСНОВЕ СЕТЕВОГО ТРАФИКА

**Филонов Артём Владимирович, Катасонов Александр Игоревич**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mails: artemfilonow@gmail.com, ksasha716@yandex.ru

**Аннотация.** Рассматриваются методы применения искусственных нейронных сетей для обнаружения атак в сфере кибербезопасности.

**Ключевые слова:** архитектура ИНС; обнаружение сетевых атак; машинное обучение; глубокое обучение; многослойный Персептрон; сверточные нейронные сети; длинная краткосрочная память; автоэнкодеры; генеративные состязательные сети; рекурсивные нейронные сети; графовые нейронные сети.

## INFLUENCE OF ARTIFICIAL NEURAL NETWORK ARCHITECTURE ON NETWORK ATTACKS DETECTION

**Filonov Artyom, Katasonov Aleksandr**

The Bonch-Bruевич Saint Petersburg State University of Telecommunications  
22 Bolshhevikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mails: artemfilonow@gmail.com, ksasha716@yandex.ru

**Abstract.** Methods of application of artificial neural networks for detection of threats in the field of cybersecurity are considered.

**Keywords:** architecture of ANN; detection of network attacks; machine learning; deep learning; Multilayer Perceptron; Convolutional neural networks; Long short-term memory; Autoencoders; Generative adversarial networks; Recursive neural networks; Graph neural networks.

Искусственные нейронные сети (ИНС) приобрели значительную популярность в области кибербезопасности благодаря своей способности выявлять сложные закономерности и модели поведения в больших объемах данных. Архитектура ИНС является ключевым фактором, определяющим эффективность и производительность этих моделей в задачах обнаружения сетевых атак. Именно структура и особенности построения сети во многом влияют на качество выявления вредоносной активности и адаптивность к новым видам угроз.

Существует множество различных архитектур искусственных нейронных сетей, каждая из которых имеет свои специфические характеристики и сферы применения. К наиболее распространенным относятся многослойный персептрон (MLP), сверточные нейронные сети (CNN), рекуррентные нейронные сети (RNN), включая их усовершенствованные варианты с длинной краткосрочной памятью (LSTM), а также автоэнкодеры, генеративные состязательные сети (GAN), функциональные сети радиальной основы (RBFN) и рекурсивные нейронные сети (RvNN). Каждая из этих архитектур ориентирована на работу с определенным типом данных и задач [1].

Многослойный перцептрон, обладая простой структурой, хорошо подходит для задач классификации и регрессии, особенно при обработке структурированных данных. Однако он имеет ограничения при работе с последовательными и мультиструктурными данными.

Сверточные нейронные сети проявляют высокую эффективность в извлечении пространственных признаков, что делает их незаменимыми для анализа изображений и сложных визуальных паттернов в сетевом трафике, хотя их обучение требует значительных вычислительных ресурсов и большого объема обучающих данных. Рекуррентные сети и LSTM-сети предназначены для моделирования временных зависимостей, что важно при анализе последовательной информации, например, сетевых журналов или потоковых данных, но при этом они подвержены проблемам исчезающего и взрывного градиента, требующим специальных техник обучения.

Автоэнкодеры применяются для снижения размерности и обнаружения аномалий, эффективно выявляя скрытые представления данных, однако результаты их работы трудно интерпретировать, и они чувствительны к шуму [2]. Генеративные состязательные сети позволяют создавать синтетические данные для увеличения обучающих выборок и повышения обобщающей способности моделей, но обучение таких сетей является сложным и нестабильным процессом.

Радиально-базисные функциональные сети хорошо подходят для решения задач аппроксимации функций и интерполяции, однако склонны к переобучению при недостатке данных. Рекурсивные нейронные сети специализируются на обработке иерархических структур, что важно для анализа естественного языка и синтаксиса, но требуют больших вычислительных ресурсов и затрудняются с масштабированием.

Несмотря на разнообразие и потенциал архитектур ИНС, их практическое использование сопряжено с рядом проблем. Ключевыми вызовами являются трудности с подбором качественных и адекватных для обучения данных, сложность настройки параметров моделей и высокая вычислительная нагрузка. Кроме того, динамичная и постоянно изменяющаяся природа киберугроз требует от систем регулярной перенастройки и адаптации.

Для повышения эффективности применения ИНС в задачах безопасности применяются различные подходы, включая тщательную предварительную обработку данных, использование аппаратных ускорителей для снижения временных затрат на обучение, а также внедрение методов интерпретируемости и объяснимости моделей, которые помогают лучше понять поведение ИНС и повысить доверие к их решениям [3].

Таким образом, архитектура искусственной нейронной сети занимает центральное место в разработке современных методов обнаружения сетевых атак.

Понимание сильных и слабых сторон различных архитектур позволяет специалистам в области кибербезопасности выбирать наиболее подходящие модели, учитывая специфику задач, типы атак, особенности данных и технические возможности.

Постоянное развитие и совершенствование архитектур ИНС способствует созданию более устойчивых и адаптивных систем обнаружения, способных эффективно противостоять новым и сложным киберугрозам, обеспечивая тем самым надежную защиту информационной инфраструктуры.

#### СПИСОК ЛИТЕРАТУРЫ

1. Иванько А. Ф., Иванько М. А., Сизова Ю. А. Нейронные сети: общие технологические характеристики // Научное обозрение. Технические науки. 2019. № 2. С. 17-23.
2. Басс Л. П., Кузьмина М. Г., Николаева О. В. Сверточные нейронные сети с глубоким обучением в задачах обработки гиперспектральных спутниковых данных // Препринты Института прикладной математики им. МВ Келдыша РАН. 2018. С. 282-32.
3. Ахметзянов К. Р. и др. Оптимизация вычислений нейронной сети // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. 2020. № 36. С. 117-130.

УДК: 004.056

#### ПРИМЕНЕНИЕ МЕТОДА EOF ДЛЯ СОКРЫТИЯ ДАННЫХ В ИЗОБРАЖЕНИЯХ: ВОЗМОЖНОСТИ И ОГРАНИЧЕНИЯ

**Химич Давид Станиславович**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mail: davidhimich@yandex.ru

**Аннотация.** В тезисах рассматривается метод сокрытия информации в изображениях на основе подхода EOF (End of File), при котором данные добавляются в конец файла изображения без изменения его визуального содержимого. Метод реализован в утилите Trojan, написанной на Python. Представлен краткий анализ эффективности внедрения и устойчивости метода к внешним воздействиям. Сделан вывод о применимости метода в контролируемых условиях передачи данных.

**Ключевые слова:** стеганография; сокрытие данных; EOF; Trojan; информационная безопасность; цифровая приватность; анализ эффективности.

#### USING THE EOF METHOD TO HIDE DATA IN IMAGES: POSSIBILITIES AND LIMITATIONS

**Khimich David**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications  
22 Bolshevnikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mail: davidhimich@yandex.ru

**Abstract.** The theses consider a method of hiding information in images based on the EOF (End of File) approach, in which data is added to the end of an image file without changing its visual content. The method is implemented in the Trojan utility written in Python. A brief analysis of the effectiveness of the implementation and the method's resistance to external influences is presented. The conclusion is made about the applicability of the method in controlled conditions of data transmission.

**Keywords:** steganography; data hiding; EOF; Trojan; cybersecurity; digital privacy; performance analysis.

Современные условия развития цифровых технологий и повсеместного распространения информации делают актуальной задачу защиты и сокрытия данных.

Одним из решений этой задачи выступает стеганография — технология сокрытия информации внутри носителя (например, изображения), при этом обеспечивающая минимальное визуальное или содержательное искажение [1–3]. Среди множества методов стеганографии выделяется метод EOF (End Of File), основанный на добавлении скрытых данных в конец файла. В отличие от традиционных подходов, модифицирующих пиксели изображения, метод EOF не изменяет его визуальное восприятие [4, 5]. Это делает его особенно привлекательным в задачах временной передачи конфиденциальных данных при условии сохранения целостности файла. Метод EOF предполагает добавление полезной нагрузки в конец файла-изображения, за пределы служебной области, воспринимаемой просмотрщиками.

Большинство программ отображают изображение только до метки окончания (например, IEND в PNG), игнорируя всё, что идёт после неё [6]. В рамках работы была использована собственная утилита Trojan, реализованная на Python. Она позволяет внедрять в изображения произвольные данные — от текстов до исполняемых файлов — и извлекать их обратно. Работа осуществляется через командную строку с двумя основными режимами: embed (внедрение) и extract (извлечение). Для точного отделения скрытого содержимого используется специальная сигнатура, облегчающая восстановление данных [7].

Проведён ряд тестов, направленных на оценку эффективности метода сокрытия и устойчивости к внешним воздействиям. Внедрение данных объемом до 100 КБ прошло успешно: изображения визуально не изменялись и отображались корректно. Извлечение также происходило без ошибок при условии, что файл не подвергался изменениям. Метод продемонстрировал высокую скрытность — пользователи и ПО не замечали изменений в изображении. Однако при любых модификациях файла, таких как пересохранение через редакторы, сжатие или перекодировка, скрытая информация терялась. Это свидетельствует о низкой устойчивости метода EOF к трансформациям файлов [8].

Метод EOF прост в реализации и может применяться в задачах, требующих быстрого сокрытия информации. Однако надёжность этого метода ограничена: скрытые данные легко теряются при обработке изображения. Поэтому он подходит лишь в строго контролируемых условиях, когда гарантируется сохранение файла без изменений (например, передача через USB, архивирование, прямая передача по FTP и т.д.).

Для более устойчивых решений предпочтительны методы, основанные на модификации пикселей или использования алгоритмов LSB, которые сохраняют скрытую информацию даже при минимальных изменениях файла. Метод EOF представляет собой эффективный способ сокрытия данных без изменения визуального облика изображения. Его основное преимущество — простота и незаметность. Однако низкая устойчивость к модификациям делает его ограниченно применимым в условиях реальной цифровой среды.

Метод рекомендуется использовать в обучающих целях и в задачах временного сокрытия при строгом контроле за целостностью файлов.

#### СПИСОК ЛИТЕРАТУРЫ

1. Harris C.R., Millman K.J., van der Walt S.J., Brett M., Berg S., Picus M., Weckesser W., Gommers R., Peterson P., Abbasi H., Oliphant T.E., Virtanen P., Cournapeau D., Wieser E., Taylor J., Smith N.J., Kern R., Hoyer S., van Kerkwijk M.H., Haldane A. et al. (2020). стр. 357-362.
2. Красов, А. В. Разработка методики внедрения и выявления эффективности SIEM-системы в среде доверенной зоны / А. В. Красов // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2022. № 3. С. 109-120. DOI 10.37882/2223-2966.2022.03.18. EDN XYRYTI.
3. Красов, А. В. Методика выявления в доверенной зоне потенциального использования программного обеспечения по созданию нетрадиционных (стеганографических) каналов / А. В. Красов // Наука и бизнес: пути развития. 2022. № 4(130). С. 65-78. EDN YJNYVO.
4. Коржик, В. И. Обнаружение стегосистем, использующих погружение конфиденциальной информации в контуры изображения / В. И. Коржик, З. К. Нгуен, А. В. Данышина // Наукоемкие технологии в космических исследованиях Земли. 2021. Т. 13, № 5. С. 75-85. EDN COUQRN.
5. Коржик В. И., Красов А. В. Цифровая стеганография : учебник. Москва : КноРус, 2023. 324 с. ISBN 978-5-406-10970-0. EDN KNKBXU.
6. Красов, А. В. Модель нарушителя информационной безопасности, использующего стеганографические каналы взаимодействия // Наука и бизнес: пути развития. 2022. № 4(130). С. 79-88. EDN TZAHFJ.
7. Цифровая стеганография и цифровые водяные знаки / Коржик В. И., Небаева К.А., Герлинг Е. Ю. [и др.] ; под ред. В. И. Коржика. Ч. 1. СПб: СПбГУТ, 2016. 226 с. ISBN 978-5-89160-125-3. EDN WJYUGJ.
8. Цифровая стеганография и цифровые водяные знаки / Коржик В. И., Анфиногенов С. О, Кочкарев А. И. [и др.]. Ч. 2. СПб: СПбГУТ, 2017. 198 с. ISBN 978-5-89160-153-6. EDN UNUPQR.

УДК 004.057.8

#### ОБНАРУЖЕНИЕ АНОМАЛИЙ СЕТЕВОГО ТРАФИКА ПРИ ПАКЕТНОЙ ПЕРЕДАЧЕ ДАННЫХ В МОБИЛЬНЫХ СЕТЯХ PRE-5G

Черкашин Артём Игоревич

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича  
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mail: bonch210405@yandex.ru

**Аннотация.** Обнаружение и анализ сетевого трафика при пакетной передаче данных в сетях pre-5G, является важной и особенной частью по улучшению как безопасности сетей четвертого поколения, так и вносит существенный вклад в построение безопасности сетей 5G, а также следующих поколений сетей сотовой связи. Рассмотрены подходы по обнаружению аномалий, а также виды этих аномалий.

**Ключевые слова:** сети pre-5G; анализ методов; аномалии сетевого трафика; оптимизация; машинное обучение; глубокое обучение.

## DETECTION OF NETWORK TRAFFIC ANOMALIES DURING PACKET DATA TRANSMISSION IN PRE-5G MOBILE NETWORKS

**Cherkashin Artem**

The Bonch-Bruевич Saint Petersburg State University of Telecommunications

22 Bolshhevikov Av, bldg 1, St. Petersburg, 193232, Russia

e-mail: bonch210405@yandex.ru

**Abstract.** The detection and analysis of network traffic during packet data transmission in pre-5G networks is an important and special part of improving both the security of fourth-generation networks and makes a significant contribution to building the security of 5G networks, as well as the next generations of cellular networks. Approaches to detecting anomalies, as well as the types of these anomalies, are considered.

**Keywords:** pre-5G networks; analysis of methods; network traffic anomalies; optimization; machine learning; deep learning.

Обнаружение аномалий сетевого трафика в сетях pre-5G (данные сети по сути являются продолжением развития технологии в продвинутых сетях LTE-Advanced Pro, которые являются продвинутыми технологиями сетей четвертого поколения [1]) имеет свою специфику, обусловленной гибридной архитектурой и технологиями, которые превосходят сети мобильной связи 5G, но еще не реализуют его полноценно [2].

Рассмотрим особенности сетей pre-5G, влияющие на обнаружение аномалий:

1. Высокие скорости и объем данных: использование технологий вроде 256-QAM, 4x4 MIMO и агрегации несущих приводит к значительному росту объема трафика. Системы обнаружения аномалий должны работать с этими большими данными в режиме, близком к реальному времени [4].

2. Гибридная архитектура (NSA-Non-Standalone): В сетях pre-5G радиосеть New Radio (NR) работает в паре с ядром сети LTE (EPC-Evolved Packet Core). Это создает дополнительные точки мониторинга и потенциальные уязвимости. Например: трафик разделяется между eNodeB(4G) и gNodeB(5G), необходимо контролировать как радиоканал, так и ядро сети и т.д.

3. Массовый MIMO (mMIMO): Эта технология, часто используется в pre-5G, создает множество направленных лучей к пользователям. Аномалией здесь может быть не только атака, но и аномальное поведение других факторов (например, создание помех соседним сотам).

4. Разновидность трафика. Сеть состоит из макросот, микросот, пикосот и фемтосот. Трафик в каждой из них имеет разные профили, что требует адаптивных или отдельных моделей для обнаружения аномалий.

Приведем типы аномалий, характерных для сетей pre-5G: атаки на радиоканал (намеренное создание помех в определенном частотном диапазоне), атаки на управляющие сигналы (эксплуатация уязвимостей в сигнализации, например в NAS), аномалии производительности (не вызванные злым умыслом, но указывающие на сбои в оборудовании или ПО), DDoS-атаки (массовые атаки, направленные на переполнение канала или ресурсов сети) и атаки на ядро сети (использование гибридности архитектуры NSA для атак на стыке технологий).

Рассмотрим подходы к обнаружению аномалий. Для эффективного обнаружения аномалий в таких сложных условиях используется комбинация методов [3]:

1. Статистические методы и анализ временных рядов:

— пороговые методы: это простые, но эффективные для обнаружения резких скачков трафика (например, при DDoS). Недостатком является: высокий уровень ложных срабатываний;

— анализ временных рядов: поиск аномалий в динамике ключевых показателей эффективности (KPI): таких как уровень сигнала RSRP, качество сигнала SINR, скорость передачи данных, количество подключенных устройств, процент ошибок (BLER) [5].

2. Машинное обучение (ML) и глубинное обучение (DL). Используются разные методы применения ИИ в том числе обучение с учителем и без.

3. Анализ на основе потоков (Flow-Based Analysis). Сбор метаданных о потоках пользовательских данных с ключевых точек сети (шлюзов P-GW, S-GW и EPC). А также анализ таких параметров, как: объем пакетов/байт в потоке, географическое распределение, порты, протоколы.

Таким образом, обнаружения аномалий в сетях pre-5G — это критически важная задача для обеспечения стабильности и безопасности связи. Оно осложнено гибридной архитектурой, высокими скоростями и разновидностью трафика. Современный подход заключается в использовании гибридных систем сочетающих: потоковый анализ для быстрого обнаружения крупных DDoS-атак, методы машинного обучения для детектирования неизвестных и сложных аномалий в поведении сети и пользователей, глубокое обучение (LSTM-сети) для анализа многомерных временных рядов сетевых KPI. Такие системы становятся неотъемлемой частью

операторов связи, эволюционируя в сторону проактивного управления сетью с предсказанием сбоев и атак до того, как они окажут серьезное влияние на пользователей.

#### СПИСОК ЛИТЕРАТУРЫ

1. Тихвинский В. О., Тереньев С. В., Юрчук А. Б. Сети мобильной связи LTE // Экотрендз. 2010. С. 81.
2. Олейникова А. В., Нуртай М. Д., Шманов Н. М. Перспективы развития связи 5G // Современные материалы, техника и технологии. 2015.
3. Антонова В. М., Кондрашова Д. А., Сухорукова Н. А. Угрозы безопасности сетей 5G // ТГТУ. С. 58.
4. Раздел между mmWave и sub-6GHz [Электронный ресурс]. Режим доступа: <https://www.letemsvetemapplem.eu/ru/2020/09/07/rozdil-mezhi-mmwave-a-sub-6ghz/> (дата обращения: 07.09.2025).
5. The Analysis of Key Performance Indicators in 4G LTE Networks [Электронный ресурс]. Режим доступа: [https://www.researchgate.net/publication/335805987\\_The\\_Analysis\\_of\\_Key\\_Performance\\_Indicators\\_in\\_4GLTE\\_Networks](https://www.researchgate.net/publication/335805987_The_Analysis_of_Key_Performance_Indicators_in_4GLTE_Networks) (дата обращения: 09.09.2025).

УДК 004.056.53

#### ЭФФЕКТИВНОСТЬ WAZUH ПРИ ОБНАРУЖЕНИИ АТАК В ЛВС

**Шарифов Роман Геннадьевич**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича  
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия  
e-mail: roman14781@gmail.com

**Аннотация.** Представлена оценка обнаружения атак в компактном сегменте ЛВС на базе Wazuh. Описаны стенд, интеграция сетевых и веб-источников, пять сценариев: сетевая разведка, SSH-брутфорс, веб-сканирование, Shellshock, SQL-инъекции. Показана надёжная фиксация событий, автоматизированное реагирование с временной блокировкой источника, достаточность анализа веб-журналов.

**Ключевые слова:** SIEM-система; Wazuh; информационная безопасность; обнаружение атак; ЛВС.

#### EFFECTIVENESS OF WAZUH FOR LAN ATTACK DETECTION

**Sharifov Roman**

The Bonch-Bruevich St. Petersburg State University of Telecommunications  
22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia  
e-mail: roman14781@gmail.com

**Abstract.** An experimental assessment of attack detection in a compact LAN segment based on Wazuh is presented. The testbed, integration of network and web sources, and five scenarios are described: network reconnaissance, SSH brute force, web scanning, Shellshock, and SQL injection. Results show reliable event capture, automated response with temporary source blocking, and the sufficiency of web server log analysis.

**Keywords:** SIEM system; Wazuh; information security; attack detection; LAN.

Работа направлена на эмпирическую оценку обнаружения типовых атак в компактном сегменте локальной сети при использовании единого центра мониторинга и реагирования. В качестве ядра применяется SIEM-система Wazuh — открытая платформа, которая объединяет сбор, нормализацию и корреляцию событий, выполняет аналитические процедуры и поддерживает автоматизированное реагирование [1]. Цель состоит в формировании воспроизводимой методики и набора практических настроек для инфраструктур с ограниченными ресурсами, а также в уточнении минимально достаточной конфигурации для устойчивого мониторинга и контроля инцидентов.

Развернут изолированный стенд с одноузловой установкой Wazuh на Ubuntu и агентами на целевых узлах. На уязвимом узле развернуто учебное веб-приложение DVWA, что обеспечивает воспроизводимые условия для анализа прикладного трафика и журналов. Для сетевого уровня используется Suricata — система обнаружения и предотвращения вторжений и модуль сетевого мониторинга, который инспектирует трафик на уровне пакетов и формирует события по сигнатурам и поведенческим признакам [2]. Для прикладного уровня применяется teler — инструмент оперативного анализа журналов веб-сервера, который в реальном времени выявляет подозрительные HTTP-запросы и индикаторы компрометации и добавляет контекст к событиям [3]. Такая связка обеспечивает сквозную обработку событий от источника до аналитики и позволяет сопоставлять вклад каждого компонента в итоговый результат.

Отдельно представлена схема сегмента ЛВС с интеграцией Wazuh, отражающая размещение компонентов и потоки данных [4]. Центральное звено составляет сервер Wazuh с узлом индексирования и панелью управления, а на критических хостах установлены агенты. На периметре работает шлюз, реализующий функции системы обнаружения и предотвращения вторжений, а также межсетевого экрана веб-приложений (WAF) [5]. VPN и система управления идентификацией и доступом передают телеметрию аутентификации и удалённых сессий.

Набор сценариев включает полуоткрытое TCP SYN-сканирование, подбор паролей по SSH, веб-сканирование, попытку эксплуатации Shellshock и внедрение SQL-запросов [6]. Suricata стабильно фиксирует признаки разведки и классифицирует последовательности соединений, что дает раннее предупреждение до стадии эксплуатации [7]. Повторяющиеся ошибки входа по SSH объединяются правилами Wazuh в единый инцидент с запуском активного реагирования и временной блокировкой источника трафика. Для обнаружения веб-сканирования используется teler по записям веб-сервера: он выделяет характерные шаблоны обращений и

снижает шум легитимного трафика, что ускоряет первичную сортировку и расстановку приоритетов [8]. Обнаружение SQL-инъекций выполняется средствами Wazuh на основе журналов веб-сервера. Попытки Shellshock не приводят к компрометации, однако корректно регистрируются по характерным заголовкам HTTP и сохраняются для ретроспективного анализа [9].

Предложенная конфигурация обеспечивает целостную наблюдаемость и базовое автоматизированное реагирование, подходит для малых и средних инфраструктур и поддерживает поэтапное расширение [10–12]. Для масштабирования необходимы политика хранения и управление сроками жизни индексов, разграничение доступа на основе ролей, регулярная проверка корректности правил и документирование изменений.

#### СПИСОК ЛИТЕРАТУРЫ

1. Котенко И. В., Саенко И. Б., Юсупов Р. М. Новое поколение систем мониторинга и управления инцидентами безопасности // Информатика, телекоммуникации и управление. 2014. №3 (198) [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/novoe-pokolenie-sistem-monitoringa-i-upravleniya-incidentami-bezopasnosti> (дата обращения: 12.08.2025).
2. Documentation // Wazuh [Электронный ресурс]. URL: <https://documentation.wazuh.com/current/index.html> (дата обращения: 12.08.2025).
3. Старцев, Д. А. Некоторые особенности проектирования локальной вычислительной сети (ЛВС) и структурированной кабельной сети (СКС) среднего по размерам офиса в условиях импортозамещения / Д. А. Старцев, Г. А. Воробьев // Информационные технологии в процессе подготовки современного специалиста : Межвузовский сборник научных трудов. Том Выпуск 26. Липецк : Липецкий государственный педагогический университет имени П.П. Семенова-Тян-Шанского, 2022. С. 200–207.
4. Панькина, К. Е. Утилиты для поиска web-уязвимостей, не имеющих сигнатур / К. Е. Панькина // Инновационные, информационные и коммуникационные технологии : сборник трудов XVII Международной научно-практической конференции, Сочи, 01–10 октября 2020 года / под ред. С.У.Увайсов. Москва: Ассоциация выпускников и сотрудников ВВИА имени профессора Н.Е.Жуковского содействия сохранению исторического и научного наследия ВВИА имени профессора Н.Е. Жуковского, 2020. С. 323–327.
5. Котенко, И. В. Использование технологий больших данных для мониторинга инцидентов информационной безопасности / И. В. Котенко, И. А. Ушаков // Региональная информатика «РИ-2016» : Материалы конференции, Санкт-Петербург, 26–28 октября 2016 года. СПб.: СПОИСУ, 2016. С. 168–169. EDN OTYSRN.
6. Иванов, А. В. Исследование возможностей методики скрытого вложения цифрового водяного знака в class-файлы на виртуализированных платформах с отличающейся архитектурой / А. В. Иванов, А. В. Красов, П. И. Шариков // Научно-аналитический журнал Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. 2018. № 2. С. 79–89. EDN VKHKQU.
7. Штеренберг, С. И. Обеспечение безопасности на высокоуровневой среде Windows / С. И. Штеренберг, Г. С. Бударный, Р. Р. Ахметов // Региональная информатика (РИ-2022) : Юбилейная XVIII Санкт-Петербургская международная конференция. Материалы конференции, Санкт-Петербург, 26–28 октября 2022 года. СПб.: СПОИСУ, 2022. С. 585–586. EDN TNRPZPK.
8. Штеренберг, С. И. Анализ безопасности доменных систем / С. И. Штеренберг, Г. С. Бударный, И. В. Чумаков // Региональная информатика (РИ-2022) : Юбилейная XVIII Санкт-Петербургская международная конференция. Материалы конференции, Санкт-Петербург, 26–28 октября 2022 года. СПб.: СПОИСУ, 2022. С. 587–588. EDN EGVVUFU.
9. An approach for stego-insider detection based on a hybrid nosql database / I. Kotenko, A. Izrailov, A. Krasov, I. Ushakov // Journal of Sensor and Actuator Networks. 2021. Vol. 10, No. 2. DOI 10.3390/jsan10020025. EDN IKOMVS.
10. Хомяков, И. Н. Скрытое вложение информации в структуру байт-кода java / И. Н. Хомяков, А. В. Красов // Системы управления и информационные технологии. 2014. № 2(56). С. 89–93. EDN SEHOQF.
11. Шариков, П. И. Исследование атаки обфускацией на байт-код java-приложения с целью разрушения или повреждения цифрового водяного знака / П. И. Шариков // I-methods. 2022. Т. 14, № 1. EDN GQKQIV.
12. Разработка модели обеспечения отказоустойчивости сети передачи данных / Д. В. Сахаров, С. И. Штеренберг, М. В. Левин, Ю. А. Колесникова // Известия высших учебных заведений. Технология легкой промышленности. 2016. Т. 34, № 4. С. 14–20. EDN YNLHLN.

УДК 004.056

#### ИССЛЕДОВАНИЕ ВСТРОЕННЫХ МЕХАНИЗМОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРОГРАММНОМ ОБЕСПЕЧЕНИИ BETAFLIGHT

Янис Николай Андреевич, Румянцев Александр Дмитриевич

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Большевики пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

e-mails: [yanis20nikolay04@gmail.com](mailto:yanis20nikolay04@gmail.com), [Sasha040505@gmail.com](mailto:Sasha040505@gmail.com)

**Аннотация.** В последнее время всё больше популярности набирают беспилотные летательные аппараты (БПЛА), что делает особенно актуальным развитие методов обеспечения кибербезопасности. При этом особое внимание уделяется защите систем управления и информации устройств от несанкционированного доступа. Среди популярных открытых платформ для квадрокоптеров FPV можно выделить Betaflight. В этом исследовании рассматриваются встроенные механизмы информационной безопасности этого программного обеспечения.

**Ключевые слова:** беспилотные летательные аппараты; кибербезопасность; защита систем управления; обнаружение вторжений.

#### RESEARCH ON BUILT-IN INFORMATION SECURITY MECHANISMS IN BETAFLIGHT SOFTWARE

Yanis Nikolay, Rumyantsev Alexander

The Bonch-Bruевич Saint Petersburg State University of Telecommunications

22 Bolshhevikov Av, bldg 1, St. Petersburg, 193232, Russia

e-mails: [yanis20nikolay04@gmail.com](mailto:yanis20nikolay04@gmail.com), [Sasha040505@gmail.com](mailto:Sasha040505@gmail.com)

**Abstract.** Recently, unmanned aerial vehicles (UAVs) have been gaining increasing popularity, making the development of cybersecurity measures especially relevant. Particular attention is paid to protecting control systems and

device data from unauthorized access. Among popular open-source platforms for FPV quadcopters, Betaflight stands out. This study examines the built-in information security mechanisms of this software.

**Keywords:** unmanned aerial vehicles; cybersecurity; protection of control systems; intrusion detection.

Беспилотные летательные аппараты (БПЛА) активно используются в логистике, сельском хозяйстве, мониторинге и экстренных службах — и всё чаще становятся мишенью кибератак: перехвата управления, подмены команд, несанкционированного доступа. Betaflight — популярный open-source фреймворк [1] для FPV-БПЛА, работающий на микроконтроллерах (например, STM32) и взаимодействующий с пультом по радиоканалу [2, 3]. При подключении квадрокоптера к пульту в Betaflight применяются следующие механизмы информационной безопасности:

- привязка (bind) — создаёт уникальный защищённый радиоканал между пультом и приёмником, исключая несанкционированный доступ;
- защищённые протоколы — например, ExpressLRS с шифрованием, устойчивостью к помехам и аутентификацией через пароль (pairing word);
- failsafe аварийные действия при потере сигнала: остановка моторов, посадка или возврат домой;
- корректная настройка приёмника — предотвращает ложные команды и обеспечивает стабильность связи.

Изучая встроенные системы безопасности в Betaflight, можно определить, какие у них сильные и слабые стороны. Это особенно важно сейчас, когда киберугрозы для беспилотных летательных аппаратов только растут.

#### СПИСОК ЛИТЕРАТУРЫ

1. Kumar, P., & Singh, R. Vulnerability Assessment of Mobile Apps for Drone Control. *Journal of Cybersecurity and Privacy*, 2021, № 2(1), С. 45-58. (дата обращения: 14.09.2025).
2. Винников, С. А. Использование SDR-модуля для захвата и обработки Wi-Fi сигналов / С. А. Винников, Д. А. Красников, М. М. Ковцур // *Нанотехнологии: наука и производство*. 2025. № 3. С. 21-24. EDN XXLIJQ.
3. Ковцур, М. М. Разработка концепции защищенного централизованного взаимодействия распределенных устройств / М. М. Ковцур, А. А. Браницкий, Н. И. Казаков // *Экономика и качество систем связи*. 2023. № 2(28). С. 99-104. EDN MQUGPC.
4. Разработка методики анализа трафика сети WLAN IEEE 802.1X / Е. А. Зебзеев, Е. Ю. Герлинг, А. Ю. Киструга, М. М. Ковцур // *Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки*. 2024. № 3. С. 80-85. DOI 10.46418/2079-8199\_2024\_3\_13. EDN OSTBCQ.
5. Zhang, Y., Li, X., Wang, H., & Liu, J. Security Analysis of UAV Control Systems: Threats and Countermeasures. *IEEE Access*, 2022, № 10, С. 11234–11245. (дата обращения: 13.09.2025).



## ОГЛАВЛЕНИЕ

|                                                                                                                                                                                                                                                   |           |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>ГОСУДАРСТВЕННАЯ ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕГИОНОВ РОССИИ .....</b>                                                                                                                                                     | <b>14</b> |
| БАРЬЕРЫ ВНЕДРЕНИЯ ЦИФРОВЫХ СЕРВИСОВ В ГОССЕКТОРЕ<br>Денисов Максим Васильевич .....                                                                                                                                                               | 14        |
| СОЦИОКУЛЬТУРНЫЕ ЦЕННОСТИ ВОЕННОЙ ЖУРНАЛИСТИКИ КАК АКСИОЛОГИЧЕСКИЙ ИНСТРУМЕНТ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ<br>Ерофеева Ирина Викторовна, Михалева Людмила Игоревна .....                                                                              | 16        |
| ГОСУДАРСТВЕННЫЕ И КОРПОРАТИВНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ В УСЛОВИЯХ СОВРЕМЕННОЙ ГЕОПОЛИТИЧЕСКОЙ НЕСТАБИЛЬНОСТИ<br>Майоров Александр Владимирович .....                                                                         | 18        |
| МЕХАНИЗМЫ ЗАЩИТЫ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РЕГИОНОВ РОССИИ<br>Ренсков Дмитрий Андреевич .....                                                                                                                                     | 19        |
| ОСОБЕННОСТИ РЕАЛИЗАЦИИ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ ПО ФОРМИРОВАНИЮ ГОСУДАРСТВЕННОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ<br>Сторожик Виктор Сергеевич .....                                                                                                      | 21        |
| ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА И ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ<br>РОССИЙСКОЙ ФЕДЕРАЦИИ<br>Шилков Владимир Ильич, Гладских Марианна Владимировна .....                                                             | 23        |
| <b>ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ .....</b>                                                                                                                                                                                         | <b>26</b> |
| КЛАССИФИКАЦИЯ КРИТЕРИЕВ ОЦЕНКИ ПО РЕЗУЛЬТАТИВНОСТИ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ, КАК СОЦИАЛЬНОЙ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОЙ СИСТЕМЫ<br>Алексеев Сергей Алексеевич, Гончар Александр Михайлович ..... | 26        |
| НАЦИОНАЛЬНАЯ АНТИТЕРРОРИСТИЧЕСКАЯ БЕЗОПАСНОСТЬ<br>Алимов Денис Олегович, Кузнецов Вячеслав Дмитриевич .....                                                                                                                                       | 28        |
| ПРАВОВЫЕ ПРОБЛЕМЫ И ОРГАНИЗАЦИОННО-ТЕХНОЛОГИЧЕСКИЕ ОСОБЕННОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЧАСТНЫХ ВИРТУАЛЬНЫХ СЕТЕЙ<br>Антонова Дарья Антоновна, Шилков Владимир Ильич .....                                                                     | 29        |
| СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: МЕТОДЫ, МЕХАНИЗМЫ И СПОСОБЫ МИНИМИЗАЦИИ РИСКОВ<br>Бобонец Сергей Алексеевич, Сычев Сергей Евгеньевич .....                                                                           | 31        |
| АНОНИМНОСТЬ В СЕТИ И ЕЁ ВЛИЯНИЕ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ<br>Бобонец Сергей Алексеевич, Сычев Сергей Евгеньевич .....                                                                                                                        | 33        |
| АЛГОРИТМ ОЦЕНКИ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СИСТЕМЫ ПОЖАРНОЙ СИГНАЛИЗАЦИИ ПРИ УПРАВЛЕНИИ СИСТЕМАМИ ПОЖАРНОЙ АВТОМАТИКИ<br>Богуцкий Сергей Юрьевич, Синешук Юрий Иванович .....                                                                    | 35        |



|                                                                                                                                                                                                                                                                       |    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| ПРИМЕНЕНИЕ СПЕЦИАЛИЗИРОВАННЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ПРОВЕДЕНИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ С КУРСАНТАМИ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИ ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ РОССИЙСКОЙ ФЕДЕРАЦИИ<br>Гармаев Амгалан Алдарович, Марков Дмитрий Алексеевич ..... | 36 |
| ПЕРЕХОД С ЗАПАДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА ОТЕЧЕСТВЕННОЕ КАК ФАКТОР ПОВЫШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ<br>Грачев Михаил Иванович .....                                                                                                                        | 37 |
| ПОДГОТОВКА КУРСАНТОВ И СЛУШАТЕЛЕЙ СИСТЕМЫ МВД РОССИИ<br>Грачева Наталья Геннадьевна .....                                                                                                                                                                             | 38 |
| ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПРОВЕДЕНИИ ЗАНЯТИЙ В ВОЕННОЙ ОРДЕНА ЖУКОВА АКАДЕМИИ ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ РОССИЙСКОЙ ФЕДЕРАЦИИ<br>Григорьев Олег Вячеславович .....                                                                          | 40 |
| ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРЕПОДАВАНИИ ДИСЦИПЛИН ГУМАНИТАРНОГО ПРОФИЛЯ: ВЫЗОВЫ И ПЕРСПЕКТИВЫ<br>Евстратова Юлия Айратовна .....                                                                                                                          | 41 |
| ЭФФЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННЫХ УЧЕБНО-ТРЕНИРОВОЧНЫХ СРЕДСТВ В ПРОЦЕССЕ ОБУЧЕНИЯ КУРСАНТОВ ИНЖЕНЕРНО-ТЕХНИЧЕСКОГО ПРОФИЛЯ<br>Егоренков Сергей Александрович .....                                                                                             | 42 |
| ЭФФЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ АДДИТИВНЫХ ТЕХНОЛОГИЙ В ПРОЦЕССЕ ОБУЧЕНИЯ КУРСАНТОВ ИНЖЕНЕРНО-ТЕХНИЧЕСКОГО ПРОФИЛЯ<br>Егоренков Сергей Александрович, Егоренкова Юлия Викторовна .....                                                                                    | 43 |
| ПОВЫШЕНИЕ ЛИЧНОЙ БЕЗОПАСНОСТИ ВОЕННОСЛУЖАЩИХ ПОСРЕДСТВОМ ОРГАНИЗАЦИИ ПРОТИВОДЕЙСТВИЯ ДЕЗИНФОРМАЦИИ<br>Калкаманов Эмиль Ильясович, Донцов Иван Алексеевич .....                                                                                                        | 44 |
| ИСТОРИЧЕСКИЕ АСПЕКТЫ ВОЗНИКНОВЕНИЯ И РАЗВИТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ<br>Орехов Александр Валерьевич, Гежа Марат Анатольевич .....                                                                                                                                | 45 |
| ОСНОВНЫЕ СОСТАВЛЯЮЩИЕ, ПОСТРОЕНИЕ И ЭКСПЛУАТАЦИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ<br>Орехов Александр Валерьевич, Карсаков Никита Романович .....                                                                                                      | 46 |
| ПРИМЕНЕНИЕ АЛГОРИТМОВ И ПРОЦЕДУР ТЕОРИИ ИГР ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СТРУКТУРНЫХ ПОДРАЗДЕЛЕНИЯХ СИЛОВЫХ ВЕДОМСТВ<br>Примакин Алексей Иванович, Таратухин Никита Алексеевич .....                                                                 | 47 |
| ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТРАНСПОРТНЫХ СИСТЕМ<br>Романов Демьян Александрович .....                                                                                                                                                                     | 49 |
| ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ<br>Сейдиев Курбан Ялчинович .....                                                                                                                                                       | 50 |
| ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МЕЖВЕДОМСТВЕННОГО ВЗАИМОДЕЙСТВИЯ ЗВЕНЬЕВ РСЧС<br>Синешук Юрий Иванович, Карацев Гия Георгиевич, Каиров Заур Геннадьевич .....                                                                                        | 51 |
| ОБОСНОВАНИЕ ТРЕБОВАНИЙ К НАДЕЖНОСТИ КАК ФАКТОРУ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ ПОЖАРНОЙ АВТОМАТИКИ<br>Синешук Юрий Иванович, Кубашевская Татьяна Александровна, Лебедько Елена Николаевна .....                                                       | 52 |

|                                                                                                                                                                                                     |           |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| ГНОСЕОЛОГИЯ И ПОЗНАНИЕ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ:<br>КАК МЫ ПОЗНАЁМ КИБЕРУГРОЗЫ<br>Ставицкий Данил Владимирович, Лукьянова Александра Вячеславна .....                                    | 53        |
| ЗАЩИТА ИНФОРМАЦИИ В ВЫСШИХ ВОЕННО-ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЯХ<br>Ставицкий Данил Владимирович, Минец Вячеслав Николаевич .....                                                                      | 54        |
| ПРАВОВОЕ ОБЕСПЕЧЕНИЕ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ:<br>ОСНОВЫ, ВЫЗОВЫ И ТЕНДЕНЦИИ<br>Ставицкий Данил Владимирович, Фролова Лариса Валерьевна.....                                             | 55        |
| ОБЕСПЕЧЕНИЕ ЛИЧНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВОЕННОСЛУЖАЩИХ<br>(СОТРУДНИКОВ) СТРУКТУРНЫХ ПОДРАЗДЕЛЕНИЙ СИЛОВЫХ ВЕДОМСТВ<br>Сурков Алексеи Сергеевич, Баранов Андрей Александрович .....           | 56        |
| ПРАВОВЫЕ ПОСЛЕДСТВИЯ УТЕЧЕК ПЕРСОНАЛЬНЫХ ДАННЫХ<br>Тищенко Ирина Вячеславовна .....                                                                                                                 | 57        |
| СРАВНИТЕЛЬНЫЙ АНАЛИЗ УГОЛОВНО-ПРАВОВОЙ ЗАЩИТЫ ОТ КОМПЬЮТЕРНЫХ<br>ПРЕСТУПЛЕНИЙ В ИНДИИ И В РОССИИ<br>Хазинурова Екатерина Андреевна .....                                                            | 58        |
| <b>БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ .....</b>                                                                                                                                                 | <b>60</b> |
| ОБНАРУЖЕНИЕ АНОМАЛИЙ В ИНФОРМАЦИОННЫХ СИСТЕМАХ НА ОСНОВЕ ГЕТЕРОГЕННЫХ<br>ГРАФОВЫХ НЕЙРОННЫХ СЕТЕЙ И БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ<br>Абраменко Георгий Тимофеевич, Котенко Игорь Витальевич.....         | 60        |
| УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПОДРАЗДЕЛЕНИЯХ<br>ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ В КОНТЕКСТЕ РАЗВИТИЯ<br>И РАСПРОСТРАНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА<br>Афонин Петр Николаевич .....   | 61        |
| ПРЕДПОСЫЛКИ И НАЗНАЧЕНИЕ МОДЕЛИ ПОВЕДЕНИЯ НЕУМЫШЛЕННОГО<br>ИНСАЙДЕРА В ИНФОРМАЦИОННОЙ СИСТЕМЕ ОРГАНИЗАЦИИ<br>Буйневич Михаил Викторович, Моисеенко Григорий Юрьевич, Жернова Ксения Николаевна..... | 64        |
| АНАЛИЗ АКТИВНОСТИ ПОЛЬЗОВАТЕЛЕЙ В СОЦИАЛЬНОЙ СЕТИ «ВКОНТАКТЕ»<br>Виткова Лидия Андреевна, Лебедева Дарья Александровна .....                                                                        | 65        |
| МЕТА-МОДЕЛЬ СОТРУДНИКА ОРГАНИЗАЦИИ ДЛЯ ВЫЯВЛЕНИЯ<br>ИНСАЙДЕРСКОЙ ДЕЯТЕЛЬНОСТИ<br>Власов Дмитрий Сергеевич, Мелешко Алексей Викторович.....                                                          | 66        |
| МОДЕЛИ АТАК, СЛЕДОВ И СРЕДЫ СОВЕРШЕНИЯ ИНЦИДЕНТОВ<br>С ИСПОЛЬЗОВАНИЕМ АППАРАТА НЕЧЁТКОЙ ЛОГИКИ<br>Горда Максим Дмитриевич, Чечулин Андрей Алексеевич .....                                          | 67        |
| ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ПОВЫШЕНИЯ<br>ЭФФЕКТИВНОСТИ УПРАВЛЕНИЯ ПРЕДПРИЯТИЕМ<br>Грачев Михаил Иванович .....                                                                      | 69        |
| ИСПОЛЬЗОВАНИЕ ИИ ДЛЯ АНАЛИЗА SBOM И ТРИАЖА УЯЗВИМОСТЕЙ В ОТКРЫТОМ ПО<br>Давыдов Виталий Владимирович, Козырев Владислав Сергеевич.....                                                              | 70        |
| РАЗРАБОТКА ЗАЩИЩЕННОГО ПРОТОКОЛА ДЕЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ<br>В БЕСПРОВОДНОЙ СЕНСОРНОЙ СЕТИ<br>Десницкий Василий Алексеевич .....                                                              | 71        |
| ОЦЕНКА ИССЛЕДОВАТЕЛЬСКОГО ПРОТОТИПА САМООРГАНИЗУЮЩЕЙСЯ<br>ДЕЦЕНТРАЛИЗОВАННОЙ БЕСПРОВОДНОЙ СЕНСОРНОЙ СЕТИ<br>Десницкий Василий Алексеевич .....                                                      | 72        |

|                                                                                                                                                                                                                                                                |    |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| О ВЛИЯНИИ АРХИТЕКТУРНЫХ РЕШЕНИЙ НА БЕЗОПАСНОСТЬ ПРИНЯТИЯ РЕШЕНИЙ<br>В ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМАХ<br>Дубенецкий Владислав Алексеевич, Кузнецов Александр Григорьевич,<br>Цехановский Владислав Владимирович .....                                       | 74 |
| ВЫБОР СТЕПЕНИ РАСШИРЕНИЯ ДВОИЧНОГО ПОЛЯ ДЛЯ ЗАДАНИЯ ВЕКТОРНЫХ<br>КОНЕЧНЫХ ПОЛЕЙ КАК НОСИТЕЛЕЙ ДВУХКЛЮЧЕВЫХ КРИПТОАЛГОРИТМОВ<br>НА ТРУДНО ОБРАТИМЫХ ОТОБРАЖЕНИЯХ<br>Захаров Дмитрий Викторович, Молдовян Александр Андреевич, Молдовян Дмитрий Николаевич ..... | 75 |
| АНАЛИЗ АЛГОРИТМОВ ФЕДЕРАТИВНОЙ КЛАСТЕРИЗАЦИИ<br>Забалуев Даниил Антонович, Колпащиков Максим Алексеевич .....                                                                                                                                                  | 77 |
| КОНЕЧНЫЕ АЛГЕБРЫ МАТРИЦ КАК НОСИТЕЛИ АЛГОРИТМОВ ЭЦП<br>СО СКРЫТОЙ ГРУППОЙ<br>Захаров Дмитрий Викторович, Молдовян Дмитрий Николаевич, Молдовян Николай Андреевич .....                                                                                         | 79 |
| СОСТЯЗАТЕЛЬНЫЕ АТАКИ НА ВХОДНЫЕ ДАННЫЕ НЕЙРОННОЙ СЕТИ РАСПОЗНАВАНИЯ:<br>ТЕОРИЯ И ЭКСПЕРИМЕНТ<br>Зеленцова Елена Викторовна, Виткова Лидия Андреевна .....                                                                                                      | 81 |
| ВЫЯВЛЕНИЕ МНОГОШАГОВЫХ КИБЕРАТАК В КОМПЬЮТЕРНЫХ СЕТЯХ НА ОСНОВЕ<br>КОМБИНИРОВАНИЯ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ<br>И ОБРАБОТКИ БОЛЬШИХ ДАННЫХ<br>Зеличенко Игорь Юрьевич, Котенко Игорь Витальевич .....                                                          | 83 |
| ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОПЕРАЦИОННЫХ<br>СИСТЕМ СЕМЕЙСТВА LINUX<br>Ивакина Мария Дмитриевна, Шилков Владимир Ильич .....                                                                                                          | 85 |
| ПРОСТРАНСТВЕННАЯ КОНФИДЕНЦИАЛЬНОСТЬ: РИСКИ, МАСКИРОВАНИЕ<br>И АРХИТЕКТУРА ДОВЕРИЯ ПРИ ОБРАБОТКЕ ГЕОДАННЫХ<br>Изотов Даниил Юрьевич, Яровой Роберт Владимирович .....                                                                                           | 87 |
| УЯЗВИМОСТИ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ: ВЕКТОРЫ АТАК<br>И КОМПЛЕКСНЫЕ МЕРЫ ПРОТИВОДЕЙСТВИЯ<br>Клишин Александр Владимирович, Яровой Роберт Владимирович .....                                                                                                     | 88 |
| ГЕНЕРАТИВНЫЕ МОДЕЛИ КАК ИНСТРУМЕНТ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ:<br>УГРОЗЫ И КОНТРМЕРЫ<br>Клишин Александр Владимирович, Яровой Роберт Владимирович .....                                                                                                              | 89 |
| ОБЕЗЛИЧИВАНИЕ ДАННЫХ В БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЯХ:<br>ГРАНИЦЫ ПРИВАТНОСТИ<br>Клишин Александр Владимирович, Яровой Роберт Владимирович .....                                                                                                                     | 90 |
| ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ОБНАРУЖЕНИЯ<br>АНОМАЛИЙ В ВЕБ-ТРАФИКЕ<br>Колинко Инна Павловна .....                                                                                                                                                  | 91 |
| МЕТОД ПОВЫШЕНИЯ ПРОИЗВОДИТЕЛЬНОСТИ АЛГЕБРАИЧЕСКИХ<br>АЛГОРИТМОВ ЭЦП СО СКРЫТОЙ ГРУППОЙ<br>Костина Анна Александровна .....                                                                                                                                     | 92 |
| МЕТОДОЛОГИЯ ПОВЫШЕНИЯ ЗАЩИЩЕННОСТИ РАСПРЕДЕЛЕННОГО РЕЕСТРА<br>СИСТЕМ УМНОГО ГОРОДА<br>Крундышев Василий Михайлович, Калинин Максим Олегович .....                                                                                                              | 94 |
| СВЕДЕНИЕ ЗАДАЧИ ПРОЕКТИРОВАНИЕ ГРАФИЧЕСКИХ ИНТЕРФЕЙСОВ<br>К ОПТИМИЗАЦИОННОЙ<br>Курта Павел Александрович, Израилов Константин Евгеньевич .....                                                                                                                 | 95 |

|                                                                                                                                                                                                                           |     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| СРАВНИТЕЛЬНЫЙ АНАЛИЗ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ РАЗНОЙ РАЗМЕРНОСТИ<br>ДЛЯ ЗАДАЧИ ОБНАРУЖЕНИЯ ПОДОЗРИТЕЛЬНЫХ ПОЛЬЗОВАТЕЛЬСКИХ ЗАПРОСОВ<br>Лаврентьев Владимир Владимирович, Левшун Дмитрий Сергеевич .....                   | 97  |
| ПРОБЛЕМАТИКА БЕЗОПАСНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ<br>С ПОЗИЦИИ СИСТЕМНОГО АНАЛИЗА<br>Леонов Николай Викторович, Буйневич Михаил Викторович, Антонюк Евгений Артурович .....                                              | 99  |
| ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: РОЛЬ ТРЕБОВАНИЙ<br>И АРХИТЕКТУРЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ<br>Литвинов Евгений Николаевич, Ананьева Варвара Яновна .....                                                            | 100 |
| КОМПЛЕКСНЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ МОБИЛЬНЫХ УСТРОЙСТВ:<br>УГРОЗЫ, УЯЗВИМОСТИ, ЗАЩИТА<br>Лукашенко Василий Ильич, Яровой Роберт Владимирович .....                                                              | 101 |
| СОЗДАНИЕ НАБОРА ДАННЫХ ДЛЯ ЗАДАЧ БЕЗОПАСНОСТИ ВОДООЧИСТНЫХ СООРУЖЕНИЙ<br>Мелешко Алексей Викторович .....                                                                                                                 | 102 |
| ОБНАРУЖЕНИЕ АНОМАЛИЙ В КОНТЕЙНЕРНЫХ СИСТЕМАХ НА ОСНОВЕ<br>ПРОФИЛИРОВАНИЯ ПАРАМЕТРОВ БЕЗОПАСНОСТИ<br>Мельник Максим Владимирович, Котенко Игорь Витальевич .....                                                           | 104 |
| СПОСОБЫ УСИЛЕНИЯ РАНДОМИЗАЦИИ В АЛГЕБРАИЧЕСКИХ АЛГОРИТМАХ<br>ЦИФРОВОЙ ПОДПИСИ СО СКРЫТОЙ ГРУППОЙ<br>Морозова Елена Владимировна, Костина Анна Александровна .....                                                         | 105 |
| НОВЫЙ ТИП ПОСТКВАНТОВЫХ АЛГОРИТМОВ ЭЦП НА КОНЕЧНЫХ<br>АЛГЕБРАХ МАТРИЦ<br>Морозова Елена Владимировна, Михальченко Александра Викторовна,<br>Молдовян Николай Андреевич .....                                              | 107 |
| СБАЛАНСИРОВАННЫЕ АЛГЕБРАИЧЕСКИЕ АЛГОРИТМЫ ЭЦП, ОСНОВАННЫЕ<br>НА ВЫЧИСЛИТЕЛЬНОЙ ТРУДНОСТИ РЕШЕНИЯ БОЛЬШИХ<br>СИСТЕМ УРАВНЕНИЙ<br>Морозова Елена Владимировна, Щербаков Виктор Алексеевич, Молдовян Николай Андреевич ..... | 109 |
| ПРИМЕНЕНИЕ ОНТОЛОГИЧЕСКОГО МОДЕЛИРОВАНИЯ ДЛЯ УПРАВЛЕНИЯ<br>РИСКАМИ В ПРОМЫШЛЕННЫХ КИБЕРФИЗИЧЕСКИХ СИСТЕМАХ<br>Новикова Евгения Сергеевна, Мелешко Алексей Викторович .....                                                | 111 |
| МИНИМАЛЬНО ДОСТАТОЧНЫЕ ТРЕБОВАНИЯ ЗАЩИЩЕННОСТИ СИСТЕМ<br>ОБРАБОТКИ И ХРАНЕНИЯ БОЛЬШИХ ДАННЫХ<br>Полтавцева Мария Анатольевна, Александрова Елена Борисовна, Ворошин Евгений Александрович .....                           | 113 |
| МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БАЗ ДАННЫХ<br>Пучков Владимир Викторович, Виткова Лидия Андреевна .....                                                                                                                   | 115 |
| ЭТИЧЕСКИЙ ХАКИНГ В СТРАТЕГИИ КИБЕРБЕЗОПАСНОСТИ<br>Рябов Геннадий Анатольевич, Яровой Роберт Владимирович .....                                                                                                            | 116 |
| АНАЛИЗ ПРИМЕНЕНИЯ АВТОЭНКОДЕРОВ ДЛЯ ПОВЫШЕНИЯ ТОЧНОСТИ<br>КЛАССИФИКАЦИИ ИЗОБРАЖЕНИЙ<br>Садовников Владимир Евгеньевич, Саенко Игорь Борисович .....                                                                       | 117 |
| ОСНОВНЫЕ ХАРАКТЕРИСТИКИ И ВЫБОР ЗАЩИЩЕННЫХ ОПЕРАЦИОННЫХ СИСТЕМ<br>ДЛЯ КРИТИЧЕСКИХ ИНФРАСТРУКТУР<br>Селлер Анастасия Романовна .....                                                                                       | 118 |
| УГРОЗЫ И УЯЗВИМОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ<br>В РАСПРЕДЕЛЁННЫХ ОБЛАЧНЫХ АРХИТЕКТУРАХ<br>Сенин Олег Геннадьевич, Яровой Роберт Владимирович .....                                                                     | 120 |

|                                                                                                                                                                                              |            |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| УГРОЗЫ И ЗАЩИТА В ИНФРАСТРУКТУРЕ КОНТЕЙНЕРИЗАЦИИ:<br>АНАЛИЗ ПОДХОДОВ И ПРАКТИК БЕЗОПАСНОСТИ<br>Сенин Олег Геннадьевич, Яровой Роберт Владимирович .....                                      | 121        |
| LLM КАК ИНСТРУМЕНТ ДЕТЕКТИРОВАНИЯ И ПРОГНОЗИРОВАНИЯ КИБЕРУГРОЗ<br>Сенин Олег Геннадьевич, Яровой Роберт Владимирович .....                                                                   | 122        |
| LLM КАК ИНТЕЛЛЕКТУАЛЬНЫЙ ИНСТРУМЕНТ РЕВЕРС-ИНЖИНИРИНГА<br>ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ<br>Сенин Олег Геннадьевич, Яровой Роберт Владимирович .....                                  | 123        |
| LLM В СЛУЖБЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ПРАКТИЧЕСКИЕ СЦЕНАРИИ,<br>УЯЗВИМОСТИ И ГРАНИЦЫ ПРИМЕНИМОСТИ<br>Сенин Олег Геннадьевич, Яровой Роберт Владимирович .....                            | 124        |
| ОБНАРУЖЕНИЕ УЯЗВИМОСТЕЙ В ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ<br>НА ОСНОВЕ ОБУЧЕНИЯ С ПОДКРЕПЛЕНИЕМ<br>Слётов Максим Алексеевич, Котенко Игорь Витальевич .....                               | 125        |
| ОБНАРУЖЕНИЕ АТАК НА ВЕБ-ПРИЛОЖЕНИЯ С ИСПОЛЬЗОВАНИЕМ<br>КОМБИНИРОВАННОГО ПОДХОДА НА ОСНОВЕ MLP<br>Соболев Павел Сергеевич, Котенко Игорь Витальевич .....                                     | 126        |
| ЭВОЛЮЦИЯ ФИШИНГА: ОТ МАССОВЫХ РАССЫЛОК К АВТОНОМНЫМ ИИ-АГЕНТАМ<br>Стахов Максим Дмитриевич .....                                                                                             | 127        |
| МЕТОДЫ ШИФРОВАНИЯ С ОБЪЕДИНЕНИЕМ ПРОМЕЖУТОЧНЫХ ТЕКСТОВ<br>ПУТЕМ РЕШЕНИЯ СИСТЕМ ЛИНЕЙНЫХ УРАВНЕНИЙ В СХЕМАХ<br>ПСЕВДОВЕРОЯТНОСТНОГО ШИФРОВАНИЯ<br>Татчина Яна Александровна .....             | 129        |
| ПОДХОДЫ К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ КРОССЧЕЙН-ВЗАИМОДЕЙСТВИЯ<br>Теровец Алексей Алексеевич, Кушнир Дмитрий Викторович .....                                                                   | 131        |
| ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ ДАННЫХ В ЛОКАЛЬНЫХ СЕТЯХ<br>НА ОСНОВЕ БЛОКЧЕЙН-ТЕХНОЛОГИЙ<br>Шевяков Владислав Денисович, Саенко Игорь Борисович .....                                               | 132        |
| АНАЛИТИКА ЗАМЕНЯЕМОСТИ ОПЕРАЦИОННЫХ СИСТЕМ В ИНФОРМАТИЗАЦИИ<br>ДИСЦИПЛИН ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА<br>Широков Владимир Владимирович, Щиголева Марина Андреевна .....                         | 134        |
| ВОССТАНОВЛЕНИЕ КРИПТОГРАФИЧЕСКОГО КЛЮЧА ИЗ ИЗОБРАЖЕНИЯ РАДУЖНОЙ<br>ОБОЛОЧКИ С ИСПОЛЬЗОВАНИЕМ НЕЙРОСЕТЕВОЙ МОДЕЛИ<br>Штука Станислав Евгеньевич, Боршевников Алексей Евгеньевич .....         | 135        |
| ПРИНЦИПЫ ПОСТРОЕНИЯ ОТКАЗОУСТОЙЧИВЫХ И ЗАЩИЩЁННЫХ АРХИТЕКТУР ГИС<br>ДЛЯ ПОДДЕРЖКИ АДАПТИВНЫХ ПРОЕКТНЫХ РЕШЕНИЙ В МЧС РОССИИ<br>Грызунов Виталий Владимирович, Сагитов Азат Альфредович ..... | 137        |
| <b>ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ .....</b>                                                                                                                          | <b>139</b> |
| НАПРАВЛЕНИЯ АВТОМАТИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИ<br>В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ<br>Авраменко Владимир Семенович .....                                                                          | 139        |
| ПРОГРАММНЫЙ КОМПЛЕКС ОПРЕДЕЛЕНИЯ МЕСТОПОЛОЖЕНИЯ ИСТОЧНИКОВ<br>ВНУТРЕННИХ НАРУШЕНИЙ БЕЗОПАСНОСТИ В ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ<br>Авраменко Владимир Семенович .....                                 | 140        |

|                                                                                                                                                                                                                                                                              |     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| ПРОГНОЗИРОВАНИЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ НА ОСНОВЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ<br>Авраменко Владимир Семенович, Орлов Алексей Сергеевич .....                                                                                                    | 141 |
| ГЕОКОНТРОЛЛИНГ: ПОДХОДЫ К РЕАЛИЗАЦИИ ПОДДЕРЖКИ УПРАВЛЕНИЯ ТЕРРИТОРИАЛЬНОЙ АКТИВНОСТЬЮ<br>Звездарёв Дмитрий Валентинович, Ефремов Дмитрий Александрович, Биденко Сергей Иванович,<br>Беляев Александр Константинович .....                                                    | 143 |
| ОСОБЕННОСТИ ФУНКЦИОНИРОВАНИЯ И УСЛОВИЯ ПРИМЕНЕНИЯ СРЕДСТВ ДОВЕРЕННОЙ ЗАГРУЗКИ УРОВНЯ БАЗОВОЙ СИСТЕМЫ ВВОДА-ВЫВОДА НА АВТОМАТИЗИРОВАННЫХ РАБОЧИХ МЕСТАХ ПОЛЬЗОВАТЕЛЕЙ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ И ТЕХНОЛОГИЙ<br>Виноградов Владислав Романович, Парашук Игорь Борисович..... | 145 |
| МОДЕЛИРОВАНИЕ СОСТОЯНИЯ ВНЕШНЕЙ СРЕДЫ С ВЫЯВЛЕНИЕМ ТЕРРИТОРИЙ ОПАСНЫХ АТМОСФЕРНЫХ И ТЕХНОГЕННЫХ ВОЗДЕЙСТВИЙ<br>Глущенко Артём Геннадьевич .....                                                                                                                              | 147 |
| ГЕНЕРАТИВНЫЙ ПОДХОД К СОЗДАНИЮ АНОНИМИЗИРОВАННЫХ ЦИФРОВЫХ ДВОЙНИКОВ ТЕЛЕКОММУНИКАЦИОННЫХ БИЗНЕС-ПРОЦЕССОВ В ФОРМАТЕ ГРАФА ЗНАНИЙ<br>Головин Алексей Андреевич, Жукова Наталия Александровна .....                                                                            | 149 |
| СОВРЕМЕННЫЙ ПОДХОД К ПОСТРОЕНИЮ ПРОГРАММНО-ОПРЕДЕЛЯЕМЫХ БЕСПРОВОДНЫХ СЕТЕЙ СВЯЗИ<br>Гордеев Михаил Алексеевич, Олимпиев Алексей Александрович .....                                                                                                                          | 151 |
| ПРИМЕНЕНИЕ КВАНТОВЫХ ТЕХНОЛОГИЙ В ЦЕНТРАХ ОБРАБОТКИ ДАННЫХ<br>Грибков Владимир Александрович, Михайличенко Николай Валерьевич,<br>Титов Владимир Степанович, Шарко Геннадий Васильевич.....                                                                                  | 152 |
| ОСОБЕННОСТИ ФУНКЦИОНИРОВАНИЯ ИНТЕРНЕТА ВЕЩЕЙ В ЦЕНТРАХ ОБРАБОТКИ ДАННЫХ<br>Грибков Владимир Александрович, Михайличенко Николай Валерьевич,<br>Титов Владимир Степанович, Шарко Геннадий Васильевич.....                                                                     | 154 |
| ОБЕСПЕЧЕНИЕ УСТОЙЧИВОСТИ БЛОКЧЕЙН-СИСТЕМ К УГРОЗАМ БЕЗОПАСНОСТИ НА БАЗЕ ИНТЕГРИРОВАННОГО КОМПЛЕКСА МЕТОДОВ ЗАЩИТЫ И ВЕРИФИКАЦИИ<br>Калинин Максим Олегович, Бушмелев Артем Сергеевич.....                                                                                    | 156 |
| МОДЕЛИРОВАНИЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ С ПРИМЕНЕНИЕМ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ<br>Карганов Виталий Вячеславович .....                                                                                                                 | 159 |
| ИНФОРМАЦИОННО-ТЕОРЕТИЧЕСКИЙ АНАЛИЗ КАНАЛОВ СВЯЗИ: МЕТРИКИ ЗАЩИЩЁННОСТИ И ПРЕДЕЛЫ ПРИМЕНИМОСТИ<br>Клишин Александр Владимирович, Яровой Роберт Владимирович .....                                                                                                             | 161 |
| DDOS-АТАКИ НА ТЕЛЕКОММУНИКАЦИИ: УЯЗВИМОСТИ И СТРАТЕГИЯ ЗАЩИТЫ<br>Клишин Александр Владимирович, Яровой Роберт Владимирович .....                                                                                                                                             | 162 |
| НЕКОТОРЫЕ АСПЕКТЫ НЕОБХОДИМОСТИ МОДЕЛИРОВАНИЯ СИСТЕМ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ<br>Ковалев Игорь Станиславович, Пантюхин Олег Игоревич,<br>Логинов Вячеслав Алексеевич, Ногин Сергей Борисович.....                                                                             | 163 |
| ОЦЕНКА ЗАЩИЩЕННОСТИ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ: ОБЩИЕ ВОПРОСЫ И ДЕТАЛИЗАЦИЯ ЦЕЛЕЙ И ОБЪЕКТОВ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРИМЕРЕ СИСТЕМЫ ОЧИСТНЫХ СООРУЖЕНИЙ ВОДОКАНАЛА<br>Котенко Игорь Витальевич, Саенко Игорь Борисович, Парашук Игорь Борисович.....          | 165 |

|                                                                                                                                                                                                                                                                                                                             |     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| ДОСТУП ПОЛЬЗОВАТЕЛЕЙ К ЭЛЕКТРОННЫМ ОБРАЗОВАТЕЛЬНЫМ РЕСУРСАМ И ЭЛЕКТРОННОЙ<br>ДИДАКТИЧЕСКОЙ ИНФОРМАЦИИ ПО КАНАЛАМ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ:<br>СУЩНОСТЬ, ЦЕЛИ И КРИТЕРИИ АУДИТА БЕЗОПАСНОСТИ<br>Крюкова Елена Сергеевна, Паращук Игорь Борисович.....                                                                        | 167 |
| ПРИМЕНЕНИЕ МОБИЛЬНЫХ БАЗОВЫХ СТАНЦИЙ GSM В СОВРЕМЕННЫХ<br>СИСТЕМАХ СВЯЗИ И БЕЗОПАСНОСТИ<br>Кузоятов Владислав Валерьевич, Юдин Анатолий Алексеевич.....                                                                                                                                                                     | 169 |
| ПРОБЛЕМА ЗАЩИТЫ ОТ МНОГОХОДОВЫХ СОЦИО-ИНЖЕНЕРНЫХ АТАК.<br>АНАЛИЗ ОСНОВНЫХ ЭЛЕМЕНТОВ<br>Кюннер Андрей Павлович, Чечулин Андрей Алексеевич.....                                                                                                                                                                               | 171 |
| УСКОРЕНИЕ ТАКТИЛЬНОГО ИНТЕРНЕТА С ПОМОЩЬЮ ПРОТОКОЛА QUICK UDP INTERNET<br>CONNECTIONS: ВОПРОСЫ БЕЗОПАСНОСТИ И КОНФИДЕНЦИАЛЬНОСТИ<br>Лаута Олег Сергеевич, Митрофанов Михаил Валерьевич.....                                                                                                                                 | 173 |
| К ВОПРОСУ ПОСТРОЕНИЯ ЦИФРОВЫХ ДВОЙНИКОВ И БЫСТРОГО ПРОТОТИПИРОВАНИЯ<br>АЛГОРИТМОВ И ПРОГРАММНЫХ СРЕДСТВ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ<br>Левшун Дмитрий Сергеевич, Котенко Игорь Витальевич, Паращук Игорь Борисович.....                                                                                                    | 174 |
| К ВОПРОСУ МНОГОКРИТЕРИАЛЬНОГО АНАЛИЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ<br>СЕТЕЙ И СРЕДСТВ НА БАЗЕ ТЕХНОЛОГИИ ИНТЕРНЕТА ВЕЩЕЙ НА ОБЪЕКТАХ<br>КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ<br>Левшун Дмитрий Сергеевич, Паращук Игорь Борисович.....                                                                                                 | 176 |
| РЕАЛИЗАЦИЯ УПРАВЛЕНИЯ КИБЕРБЕЗОПАСНОСТЬЮ СЕТИ ПЕРЕДАЧИ ДАННЫХ<br>ЗА СЧЕТ СРЕДСТВ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ<br>НА ОСНОВЕ МАШИННОГО ОБУЧЕНИЯ<br>Липатников Валерий Алексеевич, Шевченко Александр Александрович,<br>Мелехов Кирилл Витальевич.....                                                                           | 178 |
| АНАЛИЗ ПОКАЗАТЕЛЕЙ БЕЗОПАСНОСТИ И РЕМОНТОПРИГОДНОСТИ ДАТА-ЦЕНТРОВ<br>КАК ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ<br>С ИСПОЛЬЗОВАНИЕМ ОНТОЛОГИЧЕСКОГО ПОДХОДА И МЕТОДОВ<br>ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ<br>Михайличенко Антон Валерьевич, Михайличенко Николай Валерьевич, Паращук Игорь Борисович..... | 180 |
| ЗАЩИЩЕННОСТЬ МЕЖМАШИННОГО ИНФОРМАЦИОННОГО ОБМЕНА МЕЖДУ<br>ЦЕНТРАМИ ОБРАБОТКИ ДАННЫХ: ПОДХОД К ГРУППИРОВКЕ ПРИЗНАКОВ<br>УГРОЗ И ТИПОЛОГИЗАЦИИ РИСКОВ<br>Михайличенко Николай Валерьевич, Паращук Игорь Борисович.....                                                                                                        | 182 |
| АНАЛИЗ БЕЗОПАСНОСТИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ<br>ДЛЯ ЗАЩИЩЕННОЙ ПЕРЕДАЧИ ДАННЫХ<br>Николаева Полина Арсеновна.....                                                                                                                                                                                                               | 184 |
| АНАЛИЗ БЕЗОПАСНОСТИ ОБЛАЧНЫХ СЕРВИСОВ И МЕТОДОВ ЗАЩИТЫ ДАННЫХ<br>Николаева Полина Арсеновна.....                                                                                                                                                                                                                            | 185 |
| ЗАЩИТА ГОЛОСОВЫХ КАНАЛОВ СВЯЗИ ОТ DEEPFAKE АТАК<br>Николаева Полина Арсеновна.....                                                                                                                                                                                                                                          | 186 |
| МЕТОДЫ МОНИТОРИНГА И ИДЕНТИФИКАЦИИ АНОМАЛЬНОГО ТРАФИКА В СЕТИ<br>Ногин Сергей Борисович, Сычёв Кирилл Валерьевич, Емельяненко Артур Геннадьевич.....                                                                                                                                                                        | 187 |
| К ВОПРОСУ МОНИТОРИНГА ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ<br>Ногин Сергей Борисович, Сычёв Кирилл Валерьевич, Емельяненко Артур Геннадьевич.....                                                                                                                                                                                  | 188 |
| ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ В УСЛОВИЯХ РАЗВИТИЯ<br>ЦИФРОВЫХ ТЕЛЕКОММУНИКАЦИЙ И ТЕХНОЛОГИИ MASV1<br>Нуралинов Азамат Алдабергенович, Маликбаев Талгат Дусентаевич.....                                                                                                                                   | 190 |

|                                                                                                                                                                                                                                                               |     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| НЕКОТОРЫЕ АСПЕКТЫ БЕЗОПАСНОГО ПОИСКА ДАННЫХ НА РЕСУРСАХ ЕДИНОЙ СИСТЕМЫ ДАТА-ЦЕНТРОВ И ОБЛАЧНЫХ ХРАНИЛИЩ КАК КЛЮЧЕВОГО ЭЛЕМЕНТА ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ДОЛЖНОСТНЫХ ЛИЦ<br>Осадчий Александр Иванович, Попков Юрий Алексеевич, Носов Михаил Иванович ..... | 192 |
| МОНИТОРИНГ РАБОСОСНОСОБНОСТИ ТЕЛЕФОННОЙ IP-СЕТИ И ОЦЕНКИ КАЧЕСТВА ПРЕДОСТАВЛЯЕМЫХ УСЛУГ С ПОМОЩЬЮ ПОГРАММНОГО МОДУЛЯ В УСЛОВИЯХ КИБЕРАТАК<br>Привалов Андрей Андреевич, Титов Даниил Дмитриевич, Боботина Полина Александровна.....                           | 194 |
| ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ОБРАБОТКИ ДАННЫХ<br>Ренсков Андрей Анатольевич, Ренсков Дмитрий Андреевич .....                                                                                                                             | 196 |
| ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ И МЕТОДОВ КИБЕРБЕЗОПАСНОСТИ ДЛЯ ЗАЩИТЫ РЕГИОНАЛЬНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ<br>Ренсков Дмитрий Андреевич.....                                                                                                              | 198 |
| ЗАДАЧИ, ЭТАПЫ И МЕТОДЫ ОБЕСПЕЧЕНИЯ АНАЛИЗА ЗАЩИЩЕННОСТИ ВЕДОМСТВЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ПРИ ИХ РАБОТЕ С СЕТЬЮ ОБЩЕГО ПОЛЬЗОВАНИЯ<br>Рябов Геннадий Анатольевич, Парашук Игорь Борисович.....                              | 201 |
| АНАЛИЗ ОБЩИХ И СПЕЦИАЛЬНЫХ ТРЕБОВАНИЙ К СИСТЕМЕ ОБНАРУЖЕНИЯ ВРЕДНОСНОЙ АКТИВНОСТИ В ТРАФИКЕ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ ИНДУСТРИАЛЬНОГО УМНОГО ГОРОДА<br>Саенко Игорь Борисович, Котенко Игорь Витальевич, Парашук Игорь Борисович.....               | 203 |
| ВАРИАНТ ПОВЫШЕНИЯ СКРЫТНОСТИ ПЕРЕДАЧИ ИНФОРМАЦИИ НА ОСНОВЕ ИЗМЕНЕНИЯ ХАОТИЧЕСКИХ СИГНАЛОВ-ПЕРЕНОСЧИКОВ<br>Сазонов Виктор Викторович, Альбадр Ходр Баракат.....                                                                                                | 205 |
| ИНТЕРФЕЙСЫ ДЛЯ РЕАЛИЗАЦИИ ПОИСКОВЫХ ЗАПРОСОВ: ФОРМУЛИРОВКА И ОБОСНОВАНИЕ МЕТРИК И СУБМЕТРИК ОЦЕНИВАНИЯ ЗАЩИЩЕННОСТИ<br>Саяркин Леонид Андреевич, Парашук Игорь Борисович, Селезнев Андрей Васильевич.....                                                     | 206 |
| ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТИ БЕСПРОВОДНОЙ ПЕРЕДАЧИ ДАННЫХ LORA<br>Сильчев Кирилл Владимирович.....                                                                                                                                            | 208 |
| ГЛУБОКОЕ ОБУЧЕНИЕ ДЛЯ ОБНАРУЖЕНИЯ АНОМАЛИЙ В СЕТЕВОМ ТРАФИКЕ<br>Ситдилов Дмитрий Сергеевич, Лещинский Богдан Сергеевич, Шевченко Александр Александрович .....                                                                                                | 209 |
| ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОММУНИКАЦИЙ ИНТЕРНЕТА ВЕЩЕЙ<br>Ситдилов Дмитрий Сергеевич, Лещинский Богдан Сергеевич, Шевченко Александр Александрович.....                                                                            | 211 |
| ОБЪЯСНИМЫЙ ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В СИСТЕМАХ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ<br>Ситдилов Дмитрий Сергеевич, Лещинский Богдан Сергеевич, Шевченко Александр Александрович .....                                                              | 212 |
| ПРАКТИКИ ДОВЕРИЯ К ML-МОДЕЛЯМ: КОНТРОЛЬ SHA-256 И СРАВНЕНИЕ ПОВЕДЕНИЯ PYTORCH И TENSORFLOW ПОСЛЕ ДЕСЕРИАЛИЗАЦИИ<br>Ситдилов Дмитрий Сергеевич, Лещинский Богдан Сергеевич, Шевченко Александр Александрович .....                                             | 214 |
| СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В ПРОГРАММНО-ОПРЕДЕЛЯЕМЫХ СЕТЯХ: АНАЛИЗ СОВРЕМЕННЫХ РЕШЕНИЙ, УГРОЗ И МЕТОДОВ ЗАЩИТЫ<br>Стародубцев Юрий Иванович, Митрофанов Михаил Валерьевич .....                                                                            | 215 |
| ИНТЕРВАЛЬНАЯ ОЦЕНКА КАЧЕСТВА УПРАВЛЕНЧЕСКИХ, МЕТОДИЧЕСКИХ И ПРАКТИЧЕСКИХ НАВЫКОВ ДОЛЖНОСТНЫХ ЛИЦ ОРГАНОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ<br>Шамиев Вячеслав Александрович, Пантюхин Олег Игоревич, Парашук Игорь Борисович.....        | 216 |



|                                                                                                                                                                                                                      |            |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| РАЗРАБОТКА АНАЛИТИЧЕСКОГО АППАРАТА ДЛЯ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПРИ ПЛАНИРОВАНИИ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ<br>Шарко Геннадий Васильевич, Шарко Тамара Валентиновна .....                                        | 218        |
| <b>ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ .....</b>                                                                                                                                                                | <b>221</b> |
| ВЛИЯНИЕ ИМПОРТОЗАМЕЩЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА УРОВЕНЬ<br>ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ<br>ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ<br>Аминов Хахимджон Иномджонович, Лескова Елизавета Михайловна .....            | 221        |
| ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ АПК В УСЛОВИЯХ ЦИФРОВОЙ<br>ТРАНСФОРМАЦИИ НА ПРИМЕРЕ КРАСНОДАРСКОГО КРАЯ<br>Аминов Хахимджон Иномджонович, Семиколенных Владимир Викторович .....                            | 222        |
| ВЛИЯНИЕ МЕРОПРИЯТИЙ ПО КИБЕРБЕЗОПАСНОСТИ НА ЭКОНОМИЧЕСКУЮ<br>УСТОЙЧИВОСТЬ КОМПАНИИ<br>Андреевский Игорь Леонидович, Кузнецова Ольга Борисовна .....                                                                  | 224        |
| УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПОСТРОЕНИИ<br>КОРПОРАТИВНОГО ОБЛАЧНОГО АНАЛИТИЧЕСКОГО РЕШЕНИЯ<br>Бобчинский Артем Евгеньевич, Андреевский Игорь Леонидович .....                                              | 226        |
| ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БОЛЬШИХ ДАННЫХ<br>В ЗАДАЧАХ ЭКОНОМИКИ И УПРАВЛЕНИЯ<br>Аникин Юрий Викторович, Шилков Владимир Ильич, Ивакина Мария Дмитриевна .....                                                      | 228        |
| ЦИФРОВАЯ ТРАНСФОРМАЦИЯ СИСТЕМ ВОДОСНАБЖЕНИЯ И КИБЕРБЕЗОПАСНОСТЬ<br>Аникин Юрий Викторович, Шилков Владимир Ильич .....                                                                                               | 230        |
| ОТ ИНВЕНТАРИЗАЦИИ ДО ЗАЩИТЫ ИНФОРМАЦИИ: ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ<br>ПРАКТИКИ УПРАВЛЕНИЯ ИТ-АКТИВАМИ В КОНТУРЕ<br>ИНФОРМАЦИОННО БЕЗОПАСНОСТИ<br>Василисин Павел Сергеевич .....                                        | 232        |
| КОРПОРАТИВНЫЙ ПОДХОД К ОРГАНИЗАЦИИ МНОЖЕСТВЕННОГО ДОСТУПА<br>К ИНФОКОММУНИКАЦИОННЫМ РЕСУРСАМ<br>Верзун Наталья Аркадьевна, Колбанёв Михаил Олегович, Кунтуров Андрей Леонидович .....                                | 234        |
| НЕКОТОРЫЕ АСПЕКТЫ ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ<br>ТЕХНОЛОГИЙ ТЕРМИНАЛЬНОГО ДОСТУПА<br>Емельянов Александр Александрович, Пескова Елизавета Владимировна .....                                            | 235        |
| ТРАНСПОРТНО-ЛОГИСТИЧЕСКАЯ СИСТЕМА ЭСТАКАДНОГО ТИПА UST<br>КАК СТРАТЕГИЧЕСКОЕ РЕШЕНИЕ ДЛЯ АРКТИКИ: ИНЖЕНЕРНЫЕ<br>И СОЦИАЛЬНО-ЭКОНОМИЧЕСКИЕ АСПЕКТЫ<br>Ерофеевский Даниил Владимирович, Митко Арсений Валерьевич ..... | 237        |
| ЭКОНОМИКА КИБЕРБЕЗОПАСНОСТИ — ОДИН ИЗ ПРИОРИТЕТОВ ЦИФРОВОЙ<br>ТРАНСФОРМАЦИИ ПРЕДПРИЯТИЯ<br>Коршунов Игорь Львович, Микадзе Сергей Юрьевич, Соловьева Янита Константиновна .....                                      | 239        |
| РИСКИ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЭКОНОМИКЕ<br>Коршунов Игорь Львович, Тумарев Владимир Михайлович, Шумаева Алина Денисовна .....                                                                         | 241        |
| МОДЕЛЬ ОЦЕНКИ ЦИФРОВОЙ ТРАНСФОРМАЦИИ СЕЛЬСКОГО ХОЗЯЙСТВА<br>Маслов Никита Сергеевич .....                                                                                                                            | 244        |
| МАТЕМАТИЧЕСКАЯ МОДЕЛЬ СИСТЕМЫ АКУСТИЧЕСКОГО РАСПОЗНАВАНИЯ<br>НЕИСПРАВНОСТЕЙ В РАБОТЕ ТЕХНИЧЕСКИХ ОБЪЕКТОВ<br>Верзун Наталья Аркадьевна, Колбанёв Михаил Олегович, Салиева Аделина Рустамовна .....                   | 245        |

|                                                                                                                                                                                       |            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| РАЗРАБОТКА И ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ МЕТОДА ОБУЧЕНИЯ<br>С ПОДКРЕПЛЕНИЕМ ДЛЯ ЗАДАЧ АКУСТИЧЕСКОЙ ДИАГНОСТИКИ<br>ПРОМЫШЛЕННОГО ОБОРУДОВАНИЯ<br>Салиева Аделина Рустамовна .....   | 246        |
| <b>ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТРАНСПОРТНЫХ СИСТЕМ.....</b>                                                                                                                           | <b>249</b> |
| ЭВОЛЮЦИЯ СУДОВЫХ ДВИЖИТЕЛЕЙ<br>Амелаханов Даниил Станиславович, Журавлев Антон Евгеньевич .....                                                                                       | 249        |
| ИСПОЛЬЗОВАНИЕ ТЕЛЕМАТИКИ НА ТРАНСПОРТЕ<br>Богданова Полина Вадимовна .....                                                                                                            | 251        |
| АЛГОРИТМ РАСХОЖДЕНИЯ ВСТРЕЧНЫХ СУДОВ НА ОСНОВЕ<br>МЕТОДА ПОТЕНЦИАЛЬНЫХ ПОЛЕЙ<br>Данилин Герман Владиславович, Худайназаров Юрий Кахрамонович, Соколов Сергей Сергеевич .....          | 253        |
| ОЦЕНКА ПРОИЗВОДИТЕЛЬНОСТИ АВТОМОБИЛЬНЫХ LIDAR<br>И РАДАРОВ В УСЛОВИЯХ ПЛОХОЙ ВИДИМОСТИ<br>Вавкина Елена Александровна .....                                                           | 254        |
| МЕТОДИКА ОЦЕНКИ ДОСТУПНОСТИ СИСТЕМЫ КОРПОРАТИВНОЙ СВЯЗИ СРЕДСТВАМ<br>РАДИОКОНТРОЛЯ И ТЕХНИЧЕСКОГО КОМПЬЮТЕРНОГО КОНТРОЛЯ<br>Ефанов Антон Сергеевич, Иванов Сергей Александрович ..... | 256        |
| МАШИННОЕ ЗРЕНИЕ В АВТОНОМНЫХ ТРАНСПОРТНЫХ СИСТЕМАХ:<br>УГРОЗЫ И АРХИТЕКТУРЫ ДОВЕРИЯ<br>Изотов Даниил Юрьевич, Яровой Роберт Владимирович .....                                        | 258        |
| ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ — КЛЮЧЕВОЙ ЭЛЕМЕНТ ОБЕСПЕЧЕНИЯ<br>ЖИЗНЕСПОСОБНОСТИ ЦЕПЕЙ ПОСТАВОК<br>Искандеров Юрий Марсович .....                                                       | 259        |
| ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ<br>ТРАНСПОРТНО-ЛОГИСТИЧЕСКИХ ПРОЦЕССОВ<br>Искандеров Юрий Марсович .....                                             | 261        |
| МЕТОДЫ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ЗАЩИТЫ КАНАЛОВ СВЯЗИ<br>В ИНТЕЛЛЕКТУАЛЬНЫХ ТРАНСПОРТНЫХ СИСТЕМАХ<br>Калекина Мария Александровна, Нырков Анатолий Павлович .....                        | 262        |
| АНАЛИЗ ИНСТРУМЕНТОВ ДЛЯ ПОВЫШЕНИЯ ПРОИЗВОДИТЕЛЬНОСТИ<br>РАБОЧИХ ПРОЦЕССОВ В ПОРТУ<br>Кубовский Артемий Андреевич, Журавлев Антон Евгеньевич .....                                     | 264        |
| ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БЕЗЭКИПАЖНОГО ВОДНОГО ТРАНСПОРТА<br>Нырков Анатолий Павлович, Худайназаров Юрий Кахрамонович .....                                                     | 266        |
| DEVSECOPS-ПОДХОД К РАЗРАБОТКЕ ПО ДЛЯ АВТОНОМНЫХ ТРАНСПОРТНЫХ СИСТЕМ<br>Прокопенко Даниил Николаевич .....                                                                             | 267        |
| КВАНТОВАЯ КРИПТОГРАФИЯ В БЕСПИЛОТНЫХ СИСТЕМАХ: ВЫЗОВЫ<br>И КРИТЕРИИ ОЦЕНКИ<br>Рыбакова Таисия Константиновна .....                                                                    | 269        |
| МОНИТОРИНГ ФУНКЦИОНИРОВАНИЯ БЕСПИЛОТНЫХ ТРАНСПОРТНЫХ<br>СРЕДСТВ В УСЛОВИЯХ ВНЕШНИХ ВОЗДЕЙСТВИЙ<br>Семенов Виктор Викторович .....                                                     | 271        |
| ПОВЫШЕНИЕ ЖИЗНЕСПОСОБНОСТИ СИСТЕМЫ УПРАВЛЕНИЯ МОРСКИМ ПОРТОМ<br>Хасанов Дмитрий Салимович .....                                                                                       | 272        |

|                                                                                                                                                                                                                                                                                    |            |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| АВТОМАТИЗАЦИЯ ПРОЦЕССОВ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ:<br>ВОЗМОЖНОСТИ, ОГРАНИЧЕНИЯ И ПЕРСПЕКТИВЫ РАЗВИТИЯ<br>Юмашева Елена Сергеевна .....                                                                                                                                         | 274        |
| <b>ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ<br/>И МОРСКОЙ ИНФРАСТРУКТУРЫ .....</b>                                                                                                                                                                                     | <b>277</b> |
| ИНТЕЛЛЕКТУАЛИЗАЦИЯ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПО ТЕХНОЛОГИИ<br>ЦИФРОВЫХ ДВОЙНИКОВ СИСТЕМ БОРЬБЫ ЗА ИНФОРМАЦИОННУЮ<br>ЖИВУЧЕСТЬ КОРАБЛЯ, СУДНА<br>Михальчук Андрей Васильевич, Алексеев Анатолий Владимирович, Антипов Василий Васильевич,<br>Смольников Александр Васильевич ..... | 277        |
| ЦИФРОВИЗАЦИЯ КАЧЕСТВА КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ<br>ПРИ СЕРТИФИКАЦИИ ИННОВАЦИОННЫХ РЕШЕНИЙ<br>Алексеев Анатолий Владимирович .....                                                                                                                                              | 279        |
| ИНФОРМАЦИОННАЯ ЖИВУЧЕСТЬ КОРАБЛЯ, СУДНА: МАСТЕР-КЛАСС<br>Алексеев Анатолий Владимирович .....                                                                                                                                                                                      | 281        |
| К ВОПРОСУ О РАЗРАБОТКЕ СИСТЕМЫ ДЛЯ ЭФФЕКТИВНОГО И ОБЪЕКТИВНОГО<br>РАНЖИРОВАНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ<br>Богатырёв Данил Вячеславович .....                                                                                                                                     | 283        |
| ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ СИСТЕМ УПРАВЛЕНИЯ<br>ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ<br>Вареница Лидия Андреевна .....                                                                                                                                                                   | 284        |
| ИНТЕГРАЦИЯ СНС-ТЕХНОЛОГИЙ В ЦИФРОВУЮ ЭКОСИСТЕМУ СУДОСТРОЕНИЯ<br>В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ<br>Васюкова Мария Сергеевна .....                                                                                                                                                          | 285        |
| К ВОПРОСУ О ПРАКТИЧЕСКОМ ОСВОЕНИИ СИСТЕМЫ АВТОМАТИЗИРОВАННОГО<br>ПРОЕКТИРОВАНИЯ «САПР» В ЦЕНТР СУДОРЕМОНТА АО «ЦС «ЗВЕЗДОЧКА»<br>С ПРИМЕНЕНИЕМ КВАЛИМЕТРИЧЕСКОГО РАНЖИРОВАНИЯ<br>В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ<br>Верещагин Анатолий Васильевич .....                                    | 287        |
| ОЦЕНКА ИСПОЛЬЗОВАНИЯ «РПК-КАСОР 23.5» В ОБЛАСТИ ЗАЩИТЫ ОБЪЕКТОВ<br>МОРСКОЙ ИНФРАСТРУКТУРЫ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ<br>Вчерашний Михаил Павлович .....                                                                                                                               | 288        |
| ЦИФРОВАЯ ОЦЕНКА КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ РАСПРЕДЕЛЕННОЙ<br>СИСТЕМЫ УПРАВЛЕНИЯ ФЛОТИЛИЕЙ РАЗНОРОДНЫХ СИЛ<br>Дригола Владимир Кириллович, Алексеев Анатолий Владимирович .....                                                                                                  | 290        |
| ИНФОРМАЦИОННАЯ СКРЫТНОСТЬ ГИБРИДНОЙ ЭНЕРГЕТИЧЕСКОЙ УСТАНОВКИ<br>ДЛЯ БЕСПИЛОТНЫХ НАДВОДНЫХ СУДОВ<br>Евдокимов Никита Сергеевич .....                                                                                                                                                | 292        |
| МОДЕЛИРОВАНИЕ И ПРОГНОЗИРОВАНИЕ РАСХОДА СУДОВОГО ТОПЛИВА<br>МЕТОДАМИ МАШИННОГО ОБУЧЕНИЯ<br>Ерофеевский Даниил Владимирович, Митько Арсений Валерьевич .....                                                                                                                        | 293        |
| ВНЕДРЕНИЕ ПЛАТФОРМ MDM В ЦИФРОВЫЕ ПРОЦЕССЫ СУДОСТРОИТЕЛЬНОЙ<br>ИНДУСТРИИ КАК ЭЛЕМЕНТ ЗАЩИЩЕННОЙ ЦИФРОВОЙ ТРАНСФОРМАЦИИ<br>Зиновьев Артур Георгиевич .....                                                                                                                          | 294        |
| ПОДСИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ИНТЕЛЛЕКТУАЛЬНОЙ<br>ПОДДЕРЖКИ ПЕРЕВОЗКИ НЕГАБАРИТНЫХ ГРУЗОВ<br>Илюхин Пётр Эдуардович .....                                                                                                                                             | 296        |

|                                                                                                                                                                                                                                         |     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| АКТУАЛИЗАЦИЯ БАЗЫ ДАННЫХ И ЗНАНИЙ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ<br>КЛАССА САМ С УЧЕТОМ ТРЕБОВАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ<br>Кутикова Алевтина Константиновна, Алексеев Анатолий Владимирович .....                                     | 297 |
| КОЛИЧЕСТВЕННАЯ ОЦЕНКА ЭКОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ<br>И ЗАЩИТА ДАННЫХ НА ПРИМЕРЕ АО «ЦМКБ АЛМАЗ»<br>Лихачева Елизавета Сергеевна .....                                                                                                    | 298 |
| ЗАЩИТА ОТ DDoS-АТАК В КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЕ<br>Лотоцкая Ольга Александровна .....                                                                                                                                                  | 300 |
| КОНЦЕПЦИЯ СППР ДЛЯ УПРАВЛЕНИЯ ПРОИЗВОДСТВЕННЫМИ ПРОЦЕССАМИ<br>СУДОСТРОИТЕЛЬНОГО ПРЕДПРИЯТИЯ<br>Миклуш Сергей Владимирович .....                                                                                                         | 301 |
| К ВОПРОСУ О ПРАКТИЧЕСКОМ ОСВОЕНИИ ЗАЩИЩЕННЫХ СРС-СИСТЕМ<br>В АО «СПО «АРКТИКА» С ПРИМЕНЕНИЕМ КВАЛИМЕТРИЧЕСКОГО<br>РАНЖИРОВАНИЯ<br>Миничкин Антон Алексеевич .....                                                                       | 303 |
| МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ<br>САМООРГАНИЗУЮЩИХСЯ СЕТЕЙ<br>Минкинен Артемий Александрович .....                                                                                                         | 304 |
| РАЗРАБОТКА ЭКОЛОГИЧЕСКИ БЕЗОПАСНЫХ СУДОВЫХ ДВИГАТЕЛЕЙ НА<br>АЛЬТЕРНАТИВНЫХ ВИДАХ ТОПЛИВА В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ<br>Михайлов Владимир Викторович .....                                                                                  | 305 |
| К ВОПРОСУ О РАЗРАБОТКЕ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ УПРАВЛЕНИЯ<br>БЕСПИЛОТНЫМИ СУДАМИ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ<br>Николаев Денис Сергеевич .....                                                                                             | 306 |
| АНАЛИЗ ПОДХОДОВ К СОВМЕСТНОЙ ЭКСПЛУАТАЦИИ БЕСПИЛОТНЫХ ПЛАТФОРМ<br>В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ ДЛЯ ПОИСКОВО-СПАСАТЕЛЬНЫХ<br>И ЛОГИСТИЧЕСКИХ ОПЕРАЦИЙ В АРКТИКЕ<br>Полежаев Александр Алексеевич .....                                        | 307 |
| МЕТОДЫ ОПТИМИЗАЦИЯ УПРАВЛЕНИЯ НАУЧНО-ПРОИЗВОДСТВЕННЫМ<br>ОБЪЕДИНЕНИЕМ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ<br>Рябков Яков Игоревич, Алексеев Сергей Алексеевич, Артемов Станислав Игоревич .....                                                 | 308 |
| МЕТОДОЛОГИЯ И ТЕХНОЛОГИИ ПРОАКТИВНОГО УПРАВЛЕНИЯ МОДЕРНИЗАЦИЕЙ<br>КАТАСТРОФООУСТОЙЧИВЫХ ИНФОРМАЦИОННЫХ СИСТЕМ<br>В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ<br>Савченко Максим Николаевич .....                                                            | 310 |
| К ВОПРОСУ О РАЗРАБОТКЕ КОМПЛЕКСНОЙ АВТОМАТИЗИРОВАННОЙ<br>СИСТЕМЫ МОНИТОРИНГА И ПРОГНОЗИРОВАНИЯ ТЕХНИЧЕСКОГО<br>СОСТОЯНИЯ КОРАБЕЛЬНОГО ОБОРУДОВАНИЯ<br>В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ<br>Смирнов Петр Валерьевич, Петров Валерий Петрович ..... | 312 |
| КВАЛИМЕТРИЧЕСКАЯ ОЦЕНКА СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ НА ОСНОВЕ<br>ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ОПТИМИЗАЦИИ ЗАЩИЩЕННОГО<br>УПРАВЛЕНИЯ ОБЪЕКТАМИ МОРСКОЙ ИНФРАСТРУКТУРЫ<br>Сморозин Роман Витальевич .....                          | 313 |
| К ВОПРОСУ ОБ ИМПОРТОЗАМЕЩЕНИИ В СФЕРЕ ИНФОРМАЦИОННОЙ<br>БЕЗОПАСНОСТИ РЕГИОНОВ<br>Соколов Денис Алексеевич .....                                                                                                                         | 314 |

|                                                                                                                                                                                               |            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| О РАЗРАБОТКЕ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ УПРАВЛЕНИЯ ЛОГИСТИКОЙ<br>СУДОСТРОИТЕЛЬНЫХ ПРЕДПРИЯТИЙ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ<br>Тузов Александр Владиславович .....                                    | 315        |
| РАЗРАБОТКА ЗАЩИЩЕННОЙ СИСТЕМЫ МАШИННОГО ЗРЕНИЯ ДЛЯ<br>ПРЕДОТВРАЩЕНИЯ СТОЛКНОВЕНИЙ АВТОНОМНЫХ СУДОВ<br>Чавдар Галина .....                                                                     | 316        |
| <b>ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ .....</b>                                                                                                                                       | <b>318</b> |
| ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИЕ РИСКИ ИНСТРУМЕНТАЛЬНЫХ СРЕДСТВ<br>ИСКУССТВЕННОГО ИНТЕЛЛЕКТА<br>Атышева Роза Руслановна, Шилков Владимир Ильич .....                                             | 318        |
| РАСШИРЕНИЕ ГРАНИЦ ПОНИМАНИЯ КРИТИЧЕСКОГО МЫШЛЕНИЯ В УСЛОВИЯХ<br>ЦИФРОВИЗАЦИИ СОЦИУМА И ОБРАЗОВАНИЯ<br>Баева Людмила Владимировна, Халифаева Ольга Алексеевна .....                            | 320        |
| ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ В МУЗЫКАЛЬНО-ТВОРЧЕСКОЙ<br>ДЕЯТЕЛЬНОСТИ С ИСПОЛЬЗОВАНИЕМ КЛАВИШНОГО СИНТЕЗАТОРА<br>Давлетова Клара Борисовна, Романова Наталия Александровна ..... | 321        |
| СОЦИОКУЛЬТУРНЫЕ ЦЕННОСТИ ВОЕННОЙ ЖУРНАЛИСТИКИ КАК АКСИОЛОГИЧЕСКИЙ<br>ИНСТРУМЕНТ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ<br>Ерофеева Ирина Викторовна, Михалева Людмила Игоревна .....                       | 323        |
| КОГНИТИВНЫЕ ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ<br>БЕЗОПАСНОСТИ РОССИИ<br>Кефели Игорь Федорович, Кефели Константин Игоревич .....                                                            | 325        |
| РЕЧЕВОЕ ПОВЕДЕНИЕ КАНЦЛЕРА ГЕРМАНИИ: ПРЕДПОЧТЕНИЕ — МЕНАСИВАМ<br>Мисонжников Борис Яковлевич .....                                                                                            | 327        |
| КОГНИТИВНЫЕ МЕХАНИЗМЫ СОЦИАЛЬНЫХ СИСТЕМ<br>Плебанек Ольга Васильевна .....                                                                                                                    | 329        |
| РАЗВИТИЕ КРИТИЧЕСКОГО МЫШЛЕНИЯ В УСЛОВИЯХ<br>ЦИФРОВИЗАЦИИ ОБЩЕСТВА<br>Халифаева Ольга Алексеевна .....                                                                                        | 331        |
| <b>ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОЦИОКОМПЬЮТИНГЕ .....</b>                                                                                                                                   | <b>333</b> |
| РАСПРОСТРАНЕНИЕ ФЕЙКОВОЙ ИНФОРМАЦИИ В СОЦИАЛЬНЫХ СЕТЯХ<br>НА ОСНОВЕ РАСШИРЕННОЙ МОДЕЛИ SCWIENR<br>Борисов Сергей Валерьевич .....                                                             | 333        |
| МОДЕЛЬ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОЛЬЗОВАТЕЛЯ<br>СОЦИАЛЬНОЙ СЕТИ<br>Борисов Сергей Валерьевич .....                                                                                   | 334        |
| СОЦИОКОМПЬЮТИНГ И АУДИАЛЬНЫЕ КОММУНИКАЦИИ:<br>КАК ЗАЩИЩАТЬ ГОЛОС В ЦИФРОВОЙ СРЕДЕ<br>Денисова Ольга Сергеевна .....                                                                           | 336        |
| ЛОГИСТИЧЕСКИЙ ПОРТАЛ CARGOTIME.RU: МЕТОДЫ УНИФИКАЦИИ<br>ГЕОДАННЫХ КОНТЕЙНЕРНОЙ ПЕРЕВОЗКИ<br>Есин Максим Сергеевич, Корепанова Анастасия Андреевна, Сазанов Вадим Алексеевич .....             | 337        |
| МЕТАМОДЕЛИ И МЕТРИКИ УСТОЙЧИВОСТИ СОЦИОКОМПЬЮТИНГА<br>К ИНФОРМАЦИОННЫМ ИСКАЖЕНИЯМ<br>Изотов Даниил Юрьевич, Яровой Роберт Владимирович .....                                                  | 339        |

|                                                                                                                                                                                                 |            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| СЦЕНАРНОЕ МОДЕЛИРОВАНИЕ ЭКСТРЕМАЛЬНОГО РАЗВИТИЯ ВОЛН<br>ИНФОРМАЦИОННЫХ АТАК В ВОЗМУЩЕННОМ<br>СОЦИОИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ<br>Переварюха Андрей Юрьевич .....                                | 340        |
| СЦЕНАРНОЕ МОДЕЛИРОВАНИЕ ЭКСТРЕМАЛЬНОГО РАЗВИТИЯ ВОЛН<br>ИНФОРМАЦИОННЫХ АТАК В ВОЗМУЩЕННОМ<br>СОЦИОИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ<br>Переварюха Андрей Юрьевич .....                                | 341        |
| <b>ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КИБЕРФИЗИЧЕСКИХ СИСТЕМ .....</b>                                                                                                                                 | <b>344</b> |
| ЭНЕРГОЭФФЕКТИВНОЕ И БЕЗОПАСНОЕ РАСПИСАНИЕ ПЕРЕДАЧИ ДАННЫХ<br>В КИНЕМАТИЧЕСКИХ СЕНСОРНЫХ СЕТЯХ<br>Астахова Татьяна Николаевна .....                                                              | 344        |
| ИДЕНТИФИКАЦИЯ ЛИЧНОСТИ С ИСПОЛЬЗОВАНИЕМ НЕПЕРЕДАВАЕМЫХ ТОКЕНОВ<br>Булгаков Дмитрий Алексеевич .....                                                                                             | 345        |
| ЭФФЕКТИВНОСТЬ АТАК ПО СЛОВАРЮ<br>Булгаков Дмитрий Алексеевич .....                                                                                                                              | 347        |
| РАСПОЗНОВАНИЕ ПОТЕНЦИАЛЬНО ОПАСНЫХ ПРЕДМЕТОВ В РЕАЛЬНОМ ВРЕМЕНИ<br>Головкин Матвей Максимович .....                                                                                             | 349        |
| ЦИФРОВОЙ ДВОЙНИК КАК ИСТОЧНИК РИСКОВ: НЕСОВПАДЕНИЕ С РЕАЛЬНОСТЬЮ<br>И АРХИТЕКТУРА УСТОЙЧИВОСТИ К РАСХОЖДЕНИЯМ<br>Изотов Даниил Юрьевич, Яровой Роберт Владимирович .....                        | 350        |
| ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ ЦИФРОВЫХ ДВОЙНИКОВ<br>Краснова Анна Сергеевна, Лямин Александр Сергеевич, Колбанёв Михаил Олегович .....                                                          | 351        |
| МЕТОДИКА АВТОМАТИЗАЦИИ РАЗРАБОТКИ ПРАВИЛ ОБНАРУЖЕНИЯ АТАК В SIEM<br>Малахов Максим Юрьевич, Виткова Лидия Андреевна, Нашивочников Николай Васильевич .....                                      | 352        |
| ОБНАРУЖЕНИЕ АТАК И ВИРУСОВ НА ОСНОВЕ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ<br>Пойманова Екатерина Дмитриевна .....                                                                                      | 354        |
| ОПТИМИЗАЦИЯ НЕЙРОННЫХ СЕТЕЙ ЧЕРЕЗ ПОЛУСТРУКТУРИРОВАННУЮ<br>РАЗРЕЖЕННОСТЬ АКТИВАЦИЙ<br>Раскопина Анастасия Сергеевна .....                                                                       | 355        |
| МОДЕЛИ МИГРАЦИИ В СИСТЕМАХ ХРАНЕНИЯ ДАННЫХ<br>Решетников Дмитрий Сергеевич .....                                                                                                                | 357        |
| ГЕНЕРАЦИЯ СИНТЕТИЧЕСКОГО ТРАФИКА ИНТЕРНЕТА ВЕЩЕЙ<br>ПРИ РЕШЕНИИ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ<br>Савельева Дарья Дмитриевна .....                                                           | 359        |
| АЛГОРИТМ ЗАЩИТНОГО МАСКИРОВАНИЯ АУДИОИНФОРМАЦИИ<br>С ИСПОЛЬЗОВАНИЕМ КВАЗИОРТОГОНАЛЬНЫХ МАТРИЦ<br>Сергеев Михаил Борисович, Сергеев Александр Михайлович, Григорьев Евгений Константинович ..... | 361        |
| ПРИМЕНЕНИЕ НЕЙРОННОЙ СЕТИ С АРХИТЕКТУРОЙ АВТОЭНКODЕРА<br>ДЛЯ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК<br>Татарникова Татьяна Михайловна .....                                                                   | 363        |
| ПРИМЕНЕНИЕ МЕТОДЫ ПРЕДОБРАБОТКИ ИЗОБРАЖЕНИЙ РУКОПИСНЫХ<br>ДОКУМЕНТОВ В ЗАДАЧАХ КОМПЬЮТЕРНОГО ЗРЕНИЯ<br>Шихотов Алексей Алексеевич .....                                                         | 364        |

|                                                                                                                                                                                                                                                                                               |            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| ИНТЕЛЛЕКТУАЛЬНЫЙ АНАЛИЗ ДАННЫХ О ДОРОЖНО-ТРАНСПОРТНЫХ<br>ПРОИСШЕСТВИЯХ НА ТЕРРИТОРИИ ЗАБАЙКАЛЬСКОГО КРАЯ<br>Юрко Артём Евгеньевич.....                                                                                                                                                        | 366        |
| <b>ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ.....</b>                                                                                                                                                                                                                              | <b>368</b> |
| ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ГЕОИНФОРМАЦИОННОЙ СИСТЕМЫ<br>ДЛЯ ИИ-МАРШРУТИЗАЦИИ СУДОВ В АРКТИЧЕСКИХ ВОДАХ<br>Артакин Марк Демидович, Мартын Ирма Андреевна.....                                                                                                                                 | 368        |
| ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ АРКТИЧЕСКОГО<br>МОНИТОРИНГА: ПРИМЕНЕНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ<br>БЕЗОПАСНОСТИ СУДОХОДСТВА ПО СЕВЕРНОМУ МОРСКОМУ ПУТИ<br>Болховский Илья Дмитриевич.....                                                             | 369        |
| ГЕОИНФОРМАЦИОННАЯ СИСТЕМА КАК ОСНОВА АВТОМАТИЗИРОВАННЫХ СИСТЕМ<br>УПРАВЛЕНИЯ ОПТИМАЛЬНЫМ ФУНКЦИОНИРОВАНИЕМ ЭЛЕКТРОЭНЕРГЕТИЧЕСКОЙ<br>СИСТЕМЫ В УСЛОВИЯХ ВОЗДЕЙСТВИЯ ЭКСТРЕМАЛЬНЫХ ПОГОДНЫХ ЯВЛЕНИЙ<br>Бурлов Вячеслав Георгиевич, Полюхович Максим Алексеевич, Логвинова Юлия Валерьевна ..... | 371        |
| ГЕОКОНТРОЛЛИНГОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ<br>ТЕРРИТОРИАЛЬНЫХ АКТИВНОСТЕЙ ПУБЛИЧНОЙ ВЛАСТИ В РЕГИОНЕ<br>Бурлов Вячеслав Георгиевич, Миронов Алексей Юрьевич, Миронова Анна Юрьевна .....                                                                                      | 373        |
| РАЗРАБОТКА МОДЕЛИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОПЕРАЦИОННОЙ СИСТЕМЫ<br>В КОНТУРЕ УПРАВЛЕНИЯ ГЕОИНФОРМАЦИОННОЙ СИСТЕМОЙ<br>Бурлов Вячеслав Георгиевич, Музалева Анна Юрьевна .....                                                                                                                 | 375        |
| ГЕОИНФОРМАЦИОННЫЕ СИСТЕМЫ В МОДЕЛИ ПРИНЯТИЯ УПРАВЛЕНЧЕСКИХ<br>РЕШЕНИЙ: СИСТЕМНЫЙ ПОДХОД НА ОСНОВЕ ЗАКОНА СОХРАНЕНИЯ<br>ЦЕЛОСТНОСТИ ИХ ОБЪЕКТА<br>Грачев Михаил Иванович .....                                                                                                                 | 377        |
| ПРЯМАЯ И ОБРАТНАЯ ЗАДАЧА В ВОПРОСАХ УПРАВЛЕНИЯ<br>ГЕОИНФОРМАЦИОННЫМИ СИСТЕМАМИ<br>Грачев Михаил Иванович .....                                                                                                                                                                                | 379        |
| ПРОБЛЕМЫ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ И МЕТОДЫ ИХ РЕШЕНИЯ<br>Грачев Михаил Иванович .....                                                                                                                                                                                                         | 381        |
| МОДЕЛЬ ИНТЕГРАЦИИ ГЕОДАННЫХ В OSINT<br>Грызунов Виталий Владимирович .....                                                                                                                                                                                                                    | 383        |
| УЯЗВИМОСТИ В УПРАВЛЕНИИ МОДЕЛЯМИ МАШИННОГО ОБУЧЕНИЯ<br>В ГЕОИНФОРМАЦИОННЫХ СИСТЕМАХ<br>Колбина Ольга Николаевна, Служева Маргарита Ивановна, Микуляева Анастасия Алексеевна .....                                                                                                             | 385        |
| РАЗРАБОТКА АЛГОРИТМОВ ДЛЯ КВАНТОВЫХ БАЗ ДАННЫХ В ИНФОРМАЦИОННОЙ<br>БЕЗОПАСНОСТИ<br>Колбина Ольга Николаевна, Фатин Дмитрий Романович, Федосеева Яна Артёмовна.....                                                                                                                            | 386        |
| ПРИМЕНЕНИЕ DATA SCIENCE ДЛЯ ПРОГНОЗИРОВАНИЯ<br>В ГЕОИНФОРМАЦИОННЫХ СИСТЕМАХ<br>Колбина Ольга Николаевна, Григорьева Ольга Андреевна, Лазарева Вера Дмитриевна.....                                                                                                                            | 387        |
| EDGE COMPUTING ДЛЯ IoT –УСТРОЙСТВ<br>Райан Набиль Раидович, Касумов Гамид Исакович .....                                                                                                                                                                                                      | 389        |
| ГОЛОСОВЫЕ И ЖЕСТОВЫЕ ИНТЕРФЕЙСЫ В РЕГИОНАЛЬНЫХ ГИС И СИСТЕМАХ<br>УПРАВЛЕНИЯ: РИСКИ И ЗАЩИТА<br>Пункевич Дана Марковна, Паймеров Константин Витальевич, Колбина Ольга Николаевна.....                                                                                                          | 390        |

|                                                                                                                                                                                                                                      |            |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| РОЛЬ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ В ОБЕСПЕЧЕНИИ ПРОЗРАЧНОСТИ И ДОВЕРИЯ:<br>КЕЙСЫ ИСПОЛЬЗОВАНИЯ ОТКРЫТЫХ ГЕОДАННЫХ ДЛЯ ПОЗИТИВНОГО<br>РЕПУТАЦИОННОГО ПОЗИЦИОНИРОВАНИЯ<br>Ратушняк Евгений Алексеевич, Грызунов Виталий Владимирович ..... | 392        |
| <b>ПОДГОТОВКА И ПЕРЕПОДГОТОВКА КАДРОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ<br/>ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....</b>                                                                                                                                 | <b>394</b> |
| ПРОБЛЕМАТИКА КАДРОВОГО ДЕФИЦИТА В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ<br>В РОССИИ: ВЫЗОВЫ И ОПЫТ ПРАКТИКО-ОРИЕНТИРОВАННОЙ<br>ПОДГОТОВКИ СПЕЦИАЛИСТОВ<br>Ахрамеева Ксения Андреевна .....                                                     | 394        |
| ЦИФРОВАЯ ГРАМОТНОСТЬ КАК ОСНОВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ<br>ПОЛЬЗОВАТЕЛЯ В СОВРЕМЕННОМ ОБЩЕСТВЕ<br>Борщенко Виктор Владимирович .....                                                                                             | 395        |
| ОБРАБОТКА ДАННЫХ С БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ<br>Грачев Александр Михайлович.....                                                                                                                                             | 398        |
| ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ В МУЗЫКАЛЬНО-ТВОРЧЕСКОЙ<br>ДЕЯТЕЛЬНОСТИ С ИСПОЛЬЗОВАНИЕМ КЛАВИШНОГО СИНТЕЗАТОРА<br>Давлетова Клара Борисовна, Романова Наталия Александровна .....                                        | 400        |
| ИНТЕГРАЦИЯ САУНД-ДИЗАЙНА В ОБРАЗОВАТЕЛЬНЫЕ ПРОГРАММЫ:<br>КОЛЛЕКТИВНОЕ ЦИФРОВОЕ ТВОРЧЕСТВО И СОЦИОКОМПЬЮТИНГ<br>Дельцова Наталья Сергеевна.....                                                                                       | 403        |
| ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МУЗЫКАЛЬНОМ ОБРАЗОВАНИИ<br>Денисова Ольга Сергеевна.....                                                                                                                                   | 405        |
| ГЕНЕРАЦИЯ УЧЕБНЫХ МАТЕРИАЛОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ<br>С ПОМОЩЬЮ ЯЗЫКОВЫХ МОДЕЛЕЙ<br>Карганов Виталий Вячеславович, Яровой Роберт Владимирович.....                                                                   | 406        |
| РАЗРАБОТКА КУРСА «ПРИЕМЫ РАСПОЗНАВАНИЯ И МЕРЫ ЗАЩИТЫ ОТ ТЕЛЕФОННОГО<br>МОШЕННИЧЕСТВА» ДЛЯ ПЕРЕПОДГОТОВКИ КАДРОВ<br>ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЙ<br>Ковганко Валерия Егоровна .....                                                     | 407        |
| АВТОМАТИЗАЦИЯ БИЗНЕС-ПРОЦЕССОВ В СТУДИЯХ ЗВУКОЗАПИСИ: ВНЕДРЕНИЕ<br>ЧАТ-БОТОВ И ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ<br>Мухин Максим Витальевич, Титова Розалия Андреевна .....                                                        | 408        |
| ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ОБРАЗОВАНИИ: ПОДГОТОВКА КАДРОВ<br>ДЛЯ ЦИФРОВОЙ ЭКОНОМИКИ<br>Раковский Олег Владимирович, Аньшаков Артём Евгеньевич .....                                                                                   | 410        |
| ОБУЧЕНИЕ И ПОВЫШЕНИЕ КВАЛИФИКАЦИИ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ<br>БЕЗОПАСНОСТИ В РЕГИОНАХ РОССИИ<br>Ренсков Дмитрий Андреевич.....                                                                                                 | 411        |
| ГЕЙМИФИКАЦИЯ УЧЕБНОГО ПРОЦЕССА В ИТ-УНИВЕРСИТЕТАХ: РИСКИ ПРИМЕНЕНИЯ<br>Сморозин Геннадий Николаевич, Файзуллин Радмир Ильдарович .....                                                                                               | 413        |
| <b>МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА<br/>«ЭКОСИСТЕМА БЕЗОПАСНЫХ ГОРОДСКИХ ЦИФРОВЫХ СЕРВИСОВ» .....</b>                                                                                                                                        | <b>415</b> |
| ЦИФРОВАЯ ИНКЛЮЗИЯ И КИБЕРБЕЗОПАСНОСТЬ ДЛЯ ЛЮДЕЙ С ОСОБЕННОСТЯМИ<br>ЗДОРОВЬЯ И СОЦИОКУЛЬТУРНОЙ СРЕДЫ В РОССИИ<br>Барандова Татьяна Леонидовна.....                                                                                    | 415        |



|                                                                                                                                                                                                                        |            |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| ЦИФРОВОЕ ДОВЕРИЕ: ФАКТОРЫ УСТОЙЧИВОСТИ ВЗАИМОДЕЙСТВИЯ ГРАЖДАН<br>И ВЛАСТИ ЧЕРЕЗ ЦИФРОВЫЕ ПЛАТФОРМЫ<br>Кутепова Дарья Олеговна .....                                                                                    | 417        |
| АНАЛИЗ СОЦИАЛЬНОГО САМОЧУВСТВИЯ: КАК ЦЕНТР УПРАВЛЕНИЯ РЕГИОНОМ<br>СТАНОВИТСЯ «СИГНАЛЬНОЙ СИСТЕМОЙ» ОБЩЕСТВЕННЫХ НАСТРОЕНИЙ<br>Негуляев Станислав Владимирович .....                                                    | 418        |
| ВОСПРИЯТИЕ БЕЗОПАСНОСТИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ<br>С ИИ В КОММЕНТАРИЯХ ПОЛЬЗОВАТЕЛЕЙ<br>Низомутдинов Борис Абдуллохонович .....                                                                                           | 420        |
| ИСПОЛЬЗОВАНИЕ МЕТОДА ВКЛЮЧЁННОГО НАБЛЮДЕНИЯ ПРИ ИЗУЧЕНИИ<br>СЕРВИСОВ ЭЛЕКТРОННОГО УЧАСТИЯ: ПЕРСПЕКТИВЫ И ОГРАНИЧЕНИЯ<br>Панфилов Георгий Олегович, Коваленко Наталия Николаевна .....                                  | 422        |
| СРАВНИТЕЛЬНЫЙ АНАЛИЗ РОССИЙСКИХ ID-КАРТ ЖИТЕЛЕЙ В КОНТЕКСТЕ<br>ПРЕДОСТАВЛЕНИЯ СОЦИАЛЬНОЙ ПОДДЕРЖКИ<br>Райц Валерий Андреевич .....                                                                                     | 424        |
| <b>МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА «БЕЗОПАСНЫЕ ИНТЕЛЛЕКТУАЛЬНЫЕ<br/>ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ» .....</b>                                                                                                            | <b>426</b> |
| МЕДИЦИНСКАЯ ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ДЛЯ ПЕРСОНАЛИЗИРОВАННОГО<br>ВОССТАНОВЛЕНИЯ МИМИКИ ЛИЦА ПОСЛЕ ИНСУЛЬТА<br>Авдеева Таисия Михайловна, Жаранова Анастасия Олеговна, Литвинов Владислав Леонидович .....              | 426        |
| ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ПРЕДОТВРАЩЕНИЯ МОШЕННИЧЕСКИХ ТРАНЗАКЦИЙ<br>Асадуллаев Владислав Эдуардович, Филиппов Феликс Васильевич .....                                                                                  | 428        |
| ПРОТИВОДЕЙСТВИЕ АТАКАМ ТИПА NULK В ИНФОРМАЦИОННО-<br>ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ<br>Бабанов Захар Дмитриевич, Максименко Сергей Олегович,<br>Шевченко Александр Александрович .....                                           | 429        |
| АДАПТИВНАЯ ДЕЦЕНТРАЛИЗОВАННАЯ ПЕРЕДАЧА ДАННЫХ С ФРАГМЕНТАРНЫМ<br>ШИФРОВАНИЕМ, МУЛЬТИ-МАРШРУТИЗАЦИЕЙ И СЕКТОРНОЙ АДРЕСАЦИЕЙ<br>Горохов Дмитрий Геннадьевич, Лабковская Римма Яновна .....                               | 430        |
| ОЦЕНКА ЭФФЕКТИВНОСТИ СИСТЕМ МОНИТОРИНГА И УПРАВЛЕНИЯ<br>ИНФОРМАЦИОННЫМИ СЕТЯМИ В УСЛОВИЯХ ДИНАМИЧЕСКИ<br>МЕНЯЮЩЕЙСЯ НАГРУЗКИ И ТРЕБОВАНИЙ ПОЛЬЗОВАТЕЛЕЙ<br>Губин Александр Николаевич, Климова Юлия Вячеславовна ..... | 432        |
| ИНФОРМАЦИОННАЯ ЭФФЕКТИВНОСТЬ СИСТЕМ ПОДДЕРЖКИ ИТ-ПРОЕКТОВ<br>Литвинов Владислав Леонидович, Орлова Валерия Игоревна .....                                                                                              | 433        |
| ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ОБРАЗОВАНИИ: ЭТИЧЕСКИЕ ВОПРОСЫ<br>И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ<br>Литвинов Владислав Леонидович, Самбунова Варвара Петровна .....                                                           | 434        |
| ПРИМЕНЕНИЕ ДИСТАНЦИОННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ<br>В ОБУЧЕНИИ ГРАНТОВОЙ ДЕЯТЕЛЬНОСТИ<br>Литвинов Владислав Леонидович, Литвинова Екатерина Владимировна .....                                                       | 435        |
| ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КИБЕРФИЗИЧЕСКИХ СИСТЕМ В ЭПОХУ<br>«УМНЫХ ГОРОДОВ»: АКТУАЛЬНЫЕ ПРОБЛЕМЫ РЕГУЛИРОВАНИЯ<br>Раковский Олег Владимирович, Голактионов Дмитрий Александрович .....                               | 437        |
| ОЦЕНКА ТОЧНОСТИ RSSI-МЕТОДОВ ДЛЯ ПОЗИЦИОНИРОВАНИЯ WI-FI УСТРОЙСТВ<br>Синицына Ольга Александровна, Ковцур Максим Михайлович,<br>Дрепа Владислав Евгеньевич .....                                                       | 438        |

|                                                                                                                                                                                                                             |            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| АНАЛИЗ ПРИМЕНИМОСТИ МЕТОДОВ МОДИФИКАЦИИ БАЙТ-КОДА ДЛЯ ВЛОЖЕНИЯ<br>ЦИФРОВОГО ВОДЯНОГО ЗНАКА В SCALA-ПРОГРАММЫ<br>Соколов Игорь Всеволодович .....                                                                            | 439        |
| <b>МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА «БЕЗОПАСНЫЕ СИСТЕМЫ СВЯЗИ» .....</b>                                                                                                                                                            | <b>441</b> |
| ТРУДНОСТИ ПЕРЕХОДА НА СЕТИ СВЯЗИ НОВОГО ПОКОЛЕНИЯ<br>Аветиков Артем Анатольевич, Задбоев Вадим Александрович, Тимофеев Артём Михайлович .....                                                                               | 441        |
| ОЦЕНКА ЭФФЕКТИВНОСТИ СИСТЕМЫ АВТОМАТИЗИРОВАННОГО АНАЛИЗА<br>ОКТ ИЗОБРАЖЕНИЙ<br>Аксенова Любовь Евгеньевна .....                                                                                                             | 443        |
| ФРАГМЕНТАРНОСТЬ ДАННЫХ ОБ УЯЗВИМОСТЯХ КАК ВЫЗОВ ИНФОРМАЦИОННОЙ<br>БЕЗОПАСНОСТИ И ПУТИ ЕГО ПРЕОДОЛЕНИЯ<br>Антипина Софья Олеговна, Пестов Игорь Евгеньевич .....                                                             | 444        |
| ПРЕДОТВРАЩЕНИЕ ВНЕШНИХ УТЕЧЕК ПЕРСОНАЛЬНЫХ ДАННЫХ<br>С УСТРОЙСТВ МОНИТОРИНГА ЗДОРОВЬЯ<br>Антропова Лидия Александровна, Задбоев Вадим Александрович, Санникова Полина Александровна .....                                   | 445        |
| ЭКСПЕРИМЕНТАЛЬНАЯ ОЦЕНКА СТЕПЕНИ ЗАЩИТЫ<br>KOTLIN-ПРИЛОЖЕНИЙ ПОСЛЕ ОБФУСКАЦИИ<br>Асаков Максим Рашидович .....                                                                                                              | 447        |
| АНАЛИЗ УСТОЙЧИВОСТИ ЦИФРОВЫХ ВОДЯНЫХ ЗНААКОВ В БАЙТ-КОДЕ<br>В ЗАВИСИМОСТИ ОТ ТИПА ГЕРЕНАЦИИ ЛЯМБДА-ОБЪЕКТОВ KOTLIN<br>Асаков Максим Рашидович, Рублева Екатерина Борисовна .....                                            | 449        |
| ОЦЕНКА ЭФФЕКТИВНОСТИ ANKEY SIEM NG В ОБНАРУЖЕНИИ DDOS-УГРОЗ:<br>ПОТЕНЦИАЛ И НЕДОСТАТКИ<br>Ахrameeva Ксения Андреевна, Живодовский Иван Иванович,<br>Журавлева Анастасия Сергеевна, Спицын Михаил Александрович .....        | 450        |
| ВЫБОР ПЛАТФОРМЫ ВИРТУАЛИЗАЦИИ В УСЛОВИЯХ ТЕХНОЛОГИЧЕСКОЙ ПОЛЯРИЗАЦИИ:<br>СРАВНЕНИЕ УНИВЕРСАЛЬНОГО И СПЕЦИАЛИЗИРОВАННОГО ПОДХОДОВ<br>Бирючевский Никита Евгеньевич, Пестов Игорь Евгеньевич, Мамченко Ксения Сергеевна ..... | 451        |
| ГРАФОВОЕ МОДЕЛИРОВАНИЕ СВЯЗНОСТИ УГРОЗ ДЛЯ ПРОАКТИВНОГО<br>ПРОГНОЗИРОВАНИЯ КИБЕРРИСКОВ<br>Богданов Алексей Алексеевич .....                                                                                                 | 453        |
| АВТОМАТИЗИРОВАННАЯ СИСТЕМА ДЕТЕКЦИИ УЯЗВИМОСТЕЙ<br>В IOT-УСТРОЙСТВАХ ПРОМЫШЛЕННОГО НАЗНАЧЕНИЯ<br>Борисенко Иван Иванович, Живодовский Иван Иванович, Марков Александр Сергеевич .....                                       | 454        |
| ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ПОСТКВАНТОВОЙ КРИПТОГРАФИИ В IMT-2030<br>Брюшинин Александр Юрьевич, Второв Олег Павлович, Шевченко Александр Александрович .....                                                                    | 455        |
| СИГНАЛЬНЫЙ КОНТРОЛЬ ЛИНИЙ СВЯЗИ ДЛЯ ВЫЯВЛЕНИЯ ПОДКЛЮЧЕНИЙ<br>Васичкин Сергей Сергеевич .....                                                                                                                                | 457        |
| СПЕЦИАЛИЗИРОВАННЫЕ АППАРАТНЫЕ СРЕДСТВА КАК ИНСТРУМЕНТЫ ОБЕСПЕЧЕНИЯ<br>ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БИОМЕТРИЧЕСКИХ СИСТЕМАХ<br>Веселова Анастасия Дмитриевна .....                                                          | 458        |
| ЦИФРОВАЯ УСТОЙЧИВОСТЬ ГОСУДАРСТВА ЧЕРЕЗ СОБСТВЕННЫЕ ПЛАТФОРМЫ<br>МОНИТОРИНГА БЕЗОПАСНОСТИ<br>Волостных Виктор Анатольевич, Задбоев Вадим Александрович, Липатников Валерий Алексеевич .....                                 | 460        |

|                                                                                                                                                                                                 |     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| ОСОБЕННОСТИ МАНДАТНОГО КОНТРОЛЯ ЦЕЛОСТНОСТИ В ОПЕРАЦИОННОЙ СИСТЕМЕ<br>СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ ASTRA LINUX SPECIAL EDITION<br>Гребенников Тимофей Алексеевич.....                                | 461 |
| УГРОЗЫ И МЕТОДЫ ЗАЩИТЫ ОТ АТАК ОТРАВЛЕНИЯ ДАННЫХ В СИСТЕМАХ<br>ИСКУССТВЕННОГО ИНТЕЛЛЕКТА<br>Гугунишвили Лали Джумберовна, Живодовский Иван Иванович,<br>Шулындина Мария Сергеевна.....          | 462 |
| NRD-СПИСКИ КАК КОМПОНЕНТ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ<br>Гудаков Антон Павлович, Миняев Андрей Анатольевич, Скорых Марк Андреевич.....                                                             | 464 |
| ЗАЩИТА ИНФОРМАЦИОННЫХ СИСТЕМ ОТ СЕТЕВОЙ РАЗВЕДКИ<br>МЕТОДАМИ АНАЛИЗА ТРАФИКА<br>Дзиговский Владислав Андреевич, Живодовский Иван Иванович,<br>Шадрин Илья Дмитриевич.....                       | 466 |
| ZVIRT КАК ЗАЩИЩЁННОЕ СРЕДСТВО ВИРТУАЛИЗАЦИИ<br>Дюсметова Азалия Айдаровна, Пестов Игорь Евгеньевич, Алексеева Ксения Евгеньевна.....                                                            | 467 |
| АДАПТАЦИЯ МЕТОДОЛОГИИ ЗАЩИЩЁННОЙ РАЗРАБОТКИ МОБИЛЬНЫХ<br>ПРИЛОЖЕНИЙ ДЛЯ КОМАНД РАЗНОГО МАСШТАБА<br>Емельянов Николай Романович, Ковцур Максим Михайлович.....                                   | 468 |
| ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ<br>НА ОСНОВЕ ТУМАННЫХ ВЫЧИСЛЕНИЙ<br>Задбоев Вадим Александрович, Зозуля Глеб Сергеевич.....                                                             | 469 |
| ВЛИЯНИЕ ВНЕШНИХ УГРОЗ НА ПЕРСОНАЛЬНЫЕ ДАННЫЕ<br>Задбоев Вадим Александрович, Кот Ирина Игоревна, Саитов Никита Михайлович.....                                                                  | 471 |
| ИНСТРУМЕНТ ПРОГНОЗИРОВАНИЯ АТАК ВНЕДРЕНИЯ ВРЕДОНОСНОГО<br>ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ<br>Задбоев Вадим Александрович, Липатников Валерий Алексеевич,<br>Садовников Владимир Евгеньевич.....        | 472 |
| АНАЛИЗ УЯЗВИМОСТИ MQTT В IOT<br>Задбоев Вадим Александрович, Шашин Михаил Антонович, Якобсон Дмитрий Алексеевич.....                                                                            | 474 |
| ВИРТУАЛИЗАЦИЯ МЕЖСЕТЕВЫХ ЭКРАНОВ КАК ИНСТРУМЕНТ ПОВЫШЕНИЯ<br>ОТКАЗОУСТОЙЧИВОСТИ И БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ СЕТЕЙ<br>Зуев Дмитрий Павлович.....                                                | 475 |
| БЕЗОПАСНОСТЬ НЕЙРОННЫХ СЕТЕЙ В СИСТЕМАХ КОНТРОЛЯ<br>И УПРАВЛЕНИЯ ДОСТУПОМ ТРАНСПОРТНЫХ СРЕДСТВ<br>Киркум Глеб Константинович, Сиргазинов Тимур Муратович, Шевченко Александр Александрович..... | 477 |
| ДЕКОМПОЗИЦИЯ ТРЕБОВАНИЙ ОЦЕНКИ ЗАЩИЩЕННОСТИ ОБЪЕКТА КИИ<br>ПО ФУНКЦИОНАЛЬНОМУ НАЗНАЧЕНИЮ<br>Киселёв Николай Николаевич.....                                                                     | 478 |
| ПРАКТИКА ПОСТРОЕНИЯ УСТОЙЧИВОЙ К АТАКАМ ИНФРАСТРУКТУРЫ<br>НА ОСНОВЕ ПРОТОКОЛА LORAWAN<br>Красников Даниил Андреевич, Ковцур Максим Михайлович, Никифоров Александр Вячеславович.....            | 481 |
| ГОМОМОРФНОЕ ШИФРОВАНИЕ КАК ЗАЩИТА КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ<br>Куклина Маргарита Игоревна, Романова Александра Михайловна,<br>Шевченко Александр Александрович.....                             | 482 |
| СИСТЕМЫ ПОДДЕРЖКИ КРИТИЧЕСКОЙ ОЦЕНКИ ИНФОРМАЦИИ КАК СРЕДСТВО<br>БОРЬБЫ С КОМПЬЮТЕРНЫМИ АТАКАМИ ТИПА ФИШИНГ<br>Лагутина Светлана Викторовна, Виткова Лидия Андреевна.....                        | 483 |

|                                                                                                                                                                                                                                              |     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| МЕТОДИКА ОЦЕНКИ СТОЙКОСТИ МЕТОДА ФОРМИРОВАНИЯ БИТ СЫРОГО КЛЮЧА В ПРОТОКОЛЕ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ НА ОСНОВЕ ОЦЕНКИ РАЗНОСТИ ПЕРЕДАВАЕМЫХ ОТСЧЁТОВ ПРИ ПРИМЕНЕНИИ АТАКИ НА ОСНОВЕ ПОСТРОЕНИЯ РЕШАЮЩЕЙ ТАБЛИЦЫ<br>Лапшин Алексей Сергеевич ..... | 485 |
| МОДЕЛИРОВАНИЕ СЕТЕВОГО ПОВЕДЕНИЯ КЛИЕНТСКИХ ОС<br>ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ IDS<br>Легкодымов Даниил Михайлович, Староверов Андрей Игоревич,<br>Шевченко Александр Александрович, Щёголев Ефим Константинович.....                         | 486 |
| ОЦЕНКА БЕЗОПАСНОСТИ МОДЕЛИ РАЗГРАНИЧЕНИЯ ДОСТУПА В KUBERNETES:<br>ОТ АУДИТА КОНФИГУРАЦИЙ К ПОИСКУ ВЕКТОРОВ АТАК<br>Мастеница Евгений Александрович .....                                                                                     | 487 |
| МЕТОДЫ СТАТИЧЕСКОГО АНАЛИЗА ДЛЯ ВЫЯВЛЕНИЯ ДЕФЕКТОВ<br>И УЛУЧШЕНИЯ ЧИСТОТЫ КОДА<br>Орлова Дарья Алексеевна .....                                                                                                                              | 489 |
| ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИОТ В СЕТЯХ 6G<br>Пивоваров Даниил Сергеевич, Тимофеев Лавр Алексеевич, Шевченко Александр Александрович.....                                                                                                    | 490 |
| ИССЛЕДОВАНИЕ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ КАК ТЕХНОЛОГИИ<br>ДЛЯ АВТОМАТИЗИРОВАННОГО РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ<br>Платонов Алексей Евгеньевич, Ковцур Максим Михайлович, Миняев Андрей Анатольевич .....                                           | 491 |
| ИНТЕГРАЦИЯ КОНЦЕПЦИЙ «УМНОГО ПРОИЗВОДСТВА»<br>И КИБЕРБЕЗОПАСНОСТИ В АСУ ТП<br>Повышев Сергей Алексеевич, Штеренберг Станислав Игоревич.....                                                                                                  | 492 |
| КОНЕЧНЫЕ АВТОМАТЫ В СИСТЕМАХ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ: ФОРМАЛИЗАЦИЯ<br>ПОВЕДЕНИЯ ДЛЯ АНАЛИЗА АНОМАЛИЙ В LINUX-СРЕДАХ<br>Потемкина Юлия Фёдоровна.....                                                                                           | 494 |
| СОВРЕМЕННЫЕ ВЕКТОРЫ РАЗВИТИЯ СИСТЕМ КОНТРОЛЯ ДОСТУПА<br>В ВЕБ-ПРИЛОЖЕНИЯХ<br>Рогатых Ксения Александровна .....                                                                                                                              | 495 |
| МЕТОДИКА КОМПЛЕКСНОЙ ОЦЕНКИ УРОВНЯ ЗРЕЛОСТИ СИСТЕМЫ<br>ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ<br>Сахаров Дмитрий Владимирович, Бирих Эрнест Владимирович, Гаврилов Павел Русланович .....                                                   | 496 |
| КОМПРОМИССЫ И РИСКИ ПРИ ВНЕДРЕНИИ РАСПРЕДЕЛЁННЫХ ХРАНИЛИЩ<br>В ЗАЩИЩЁННЫХ ВИРТУАЛИЗИРОВАННЫХ СРЕДАХ:<br>ОПЫТ ИСПОЛЬЗОВАНИЯ СЕРВЕРОВ В ПК СВ «БРЕСТ»<br>Строило Анна Юрьевна, Цветков Александр Юрьевич.....                                  | 499 |
| УГРОЗЫ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ АГЕНТОВ<br>ИСКУССТВЕННОГО ИНТЕЛЛЕКТА<br>Трофимов Евгений Александрович, Виткова Лидия Андреевна .....                                                                                                  | 501 |
| НОВЫЕ СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ И ДАННЫХ В СФЕРЕ<br>УСЛУГ ТЕЛЕПРИСУТСТВИЯ<br>Ушаков Игорь Александрович, Штеренберг Станислав Игоревич, Панков Арсений Владимирович .....                                                                    | 502 |
| АНАЛИЗ ВИДОВ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ОБНАРУЖЕНИЯ<br>АТАК НА ОСНОВЕ СЕТЕВОГО ТРАФИКА<br>Филонов Артём Владимирович, Катасонов Александр Игоревич.....                                                                               | 504 |
| ПРИМЕНЕНИЕ МЕТОДА EOF ДЛЯ СОКРЫТИЯ ДАННЫХ В ИЗОБРАЖЕНИЯХ:<br>ВОЗМОЖНОСТИ И ОГРАНИЧЕНИЯ<br>Химич Давид Станиславович .....                                                                                                                    | 505 |

---

|                                                                                                                                                                      |            |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| ОБНАРУЖЕНИЕ АНОМАЛИЙ СЕТЕВОГО ТРАФИКА ПРИ ПАКЕТНОЙ<br>ПЕРЕДАЧЕ ДАННЫХ В МОБИЛЬНЫХ СЕТЯХ PRE-5G<br>Черкашин Артём Игоревич.....                                       | 506        |
| ЭФФЕКТИВНОСТЬ WAZUH ПРИ ОБНАРУЖЕНИИ АТАК В ЛВС<br>Шарифов Роман Геннадьевич .....                                                                                    | 508        |
| ИССЛЕДОВАНИЕ ВСТРОЕННЫХ МЕХАНИЗМОВ ИНФОРМАЦИОННОЙ<br>БЕЗОПАСНОСТИ В ПРОГРАММНОМ ОБЕСПЕЧЕНИИ BETAFLIGHT<br>Янис Николай Андреевич, Румянцев Александр Дмитриевич..... | 509        |
| <b>ОГЛАВЛЕНИЕ.....</b>                                                                                                                                               | <b>511</b> |

## CONTENTS

|                                                                                                                                                                                                                                                      |           |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>STATE POLICY FOR ENSURING INFORMATION SECURITY<br/>IN THE REGIONS OF RUSSIA.....</b>                                                                                                                                                              | <b>14</b> |
| BARRIERS TO THE INTRODUCTION OF DIGITAL SERVICES IN THE PUBLIC SECTOR<br>Denisov Maxim .....                                                                                                                                                         | 14        |
| SOCIOCULTURAL VALUES OF MILITARY JOURNALISM AS AN AXIOLOGICAL<br>INSTRUMENT OF NATIONAL SECURITY<br>Erofeeva Irina, Lyudmila Igorevna.....                                                                                                           | 16        |
| STATE AND CORPORATE INFORMATION SYSTEMS OF THE RUSSIAN FEDERATION<br>IN THE CONTEXT OF MODERN GEO-HISTORICAL INSTABILITY<br>Mayorov Alexander .....                                                                                                  | 18        |
| MECHANISMS FOR PROTECTING THE CRITICAL INFORMATION INFRASTRUCTURE<br>OF RUSSIAN REGIONS<br>Renskov Dmitry.....                                                                                                                                       | 19        |
| THE SPECIFICS OF THE IMPLEMENTATION OF THE STATE POLICY ON THE FORMATION<br>OF THE STATE INFORMATION PROTECTION SYSTEM<br>Storozhik Viktor .....                                                                                                     | 21        |
| INFORMATION SECURITY OF THE ELECTRONIC GOVERNMENT AND STATE<br>INFORMATION SYSTEMS OF THE RUSSIAN FEDERATION<br>Shilkov Vladimir, Gladskikh Marianna.....                                                                                            | 23        |
| <b>LEGAL ASPECTS OF INFORMATION SECURITY.....</b>                                                                                                                                                                                                    | <b>26</b> |
| CLASSIFICATION OF CRITERIA FOR ASSESSING THE EFFECTIVENESS OF PROTECTING<br>CONFIDENTIAL INFORMATION IN THE STRUCTURE OF AN EDUCATIONAL<br>ORGANIZATION AS A SOCIAL ORGANIZATIONAL AND TECHNICAL SYSTEM<br>Alekseyev Sergey, Gonchar Alexander ..... | 26        |
| NATIONAL ANTI-TERRORIST SECURITY<br>Alimov Denis, Kuznetsov Veacheslav .....                                                                                                                                                                         | 28        |
| LEGAL PROBLEMS AND ORGANIZATIONAL AND TECHNOLOGICAL FEATURES<br>OF INFORMATION SECURITY OF PRIVATE VIRTUAL NETWORKS<br>Antonova Daria, Shilkov Vladimir .....                                                                                        | 29        |
| SOCIAL ENGINEERING AS A THREAT TO INFORMATION SECURITY:<br>METHODS, MECHANISMS AND WAYS TO MINIMIZE RISKS<br>Bobonets Sergey, Sychev Sergey .....                                                                                                    | 31        |
| ONLINE ANONYMITY AND ITS IMPACT ON INFORMATION SECURITY<br>Bobonets Sergey, Sychev Sergey .....                                                                                                                                                      | 33        |
| ALGORITHM FOR ASSESSING THE FUNCTIONAL SAFETY OF A FIRE ALARM SYSTEM<br>WHEN CONTROLLING FIRE AUTOMATION SYSTEMS<br>Bogutsky Sergey, Sineshchuk Yury .....                                                                                           | 35        |
| THE USE OF SPECIALIZED COMPUTER PROGRAMS TO IMPROVE THE EFFECTIVENESS<br>OF PRACTICAL TRAINING FOR CADETS OF EDUCATIONAL INSTITUTIONS<br>OF THE RUSSIAN FEDERATION NATIONAL GUARD TROOPS<br>Garmaev Amgalan, Markov Dmitry .....                     | 36        |
| TRANSITION FROM WESTERN TO DOMESTIC SOFTWARE AS A FACTOR<br>IN INCREASING INFORMATION SECURITY<br>Grachev Mikhail .....                                                                                                                              | 37        |

|                                                                                                                                                                                          |    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| TRAINING OF CADETS AND STUDENTS OF THE SYSTEM OF THE MINISTRY<br>OF INTERNAL AFFAIRS OF RUSSIA<br>Gracheva Natalia .....                                                                 | 39 |
| ISSUES OF ENSURING INFORMATION SECURITY DURING CLASSES IN THE MILITARY<br>ORDER OF ZHUKOV ACADEMY OF THE NATIONAL GUARD TROOPS<br>OF THE RUSSIAN FEDERATION<br>Grigoriev Oleg .....      | 40 |
| THE APPLICATION OF INFORMATION TECHNOLOGY IN TEACHING HUMANITIES<br>DISCIPLINES: CHALLENGES AND PROSPECTS<br>Evstratova Yuliana .....                                                    | 41 |
| THE EFFECTIVENESS OF USING ELECTRONIC EDUCATIONAL AND TRAINING TOOLS<br>IN THE PROCESS OF TRAINING CADETS OF AN ENGINEERING PROFILE<br>Egorenkov Sergey .....                            | 42 |
| EFFECTIVENESS OF USING ADDITIVE TECHNOLOGIES IN THE PROCESS<br>OF TEACHING ENGINEERING STUDENTS<br>Egorenkov Sergey, Egorenkova Julia .....                                              | 43 |
| APPLICATION OF GAME THEORY ALGORITHMS AND PROCEDURES TO ENSURING<br>INFORMATION SECURITY IN STRUCTURAL UNITS<br>OF LAW ENFORCEMENT AGENCIES<br>Kalkamanov Emil, Doncov Ivan .....        | 44 |
| HISTORICAL ASPECTS OF THE EMERGENCE AND DEVELOPMENT<br>OF INFORMATION SECURITY<br>Orechov Aleksandr, Gezha Marat .....                                                                   | 45 |
| THE MAIN COMPONENTS, CONSTRUCTION, AND OPERATION OF AN INFORMATION<br>SECURITY SYSTEM<br>Orechov Aleksandr, Karsakov Nikita .....                                                        | 46 |
| APPLICATION OF GAME THEORY ALGORITHMS AND PROCEDURES TO ENSURING<br>INFORMATION SECURITY IN STRUCTURAL UNITS OF LAW<br>ENFORCEMENT AGENCIES<br>Primakin Aleksey, Taratukhin Nikita ..... | 48 |
| INFORMATION SECURITY OF TRANSPORT SYSTEMS<br>Romanov Demyan .....                                                                                                                        | 49 |
| INFORMATION SECURITY OF MARINE EQUIPMENT<br>AND MARINE INFRASTRUCTURE OBJECTS<br>Seydiev Kurban .....                                                                                    | 50 |
| PRINCIPLES OF ENSURING INFORMATION SECURITY OF INTERDEPARTMENTAL<br>INTERACTION OF THE UNIT OF THE RSChS<br>Sineshchuk Yury, Karatsev Giya, Kairov Zaur .....                            | 51 |
| JUSTIFICATION OF REQUIREMENTS TO RELIABILITY AS A FACTOR IN ENSURING<br>INFORMATION SECURITY OF FIRE AUTOMATION SYSTEMS<br>Sineshchuk Yury, Kubashevskaya Tatyana, Lebedko Elena .....   | 52 |
| GNOSEOLOGY AND COGNITION IN THE SPHERE OF INFORMATION SECURITY:<br>HOW WE UNDERSTAND CYBER THREATS<br>Stavitsky Danil, Lukyanova Alexandra .....                                         | 53 |
| INFORMATION PROTECTION IN HIGHER MILITARY EDUCATIONAL INSTITUTIONS<br>Stavitsky Danil, Minets Vyacheslav .....                                                                           | 54 |
| LEGAL SUPPORT IN THE SPHERE OF INFORMATION SECURITY:<br>FUNDAMENTALS, CHALLENGES AND TRENDS<br>Stavitsky Danil, Frolova Larisa .....                                                     | 55 |

|                                                                                                                                                                                                                                    |           |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| ENSURING PERSONAL INFORMATION SECURITY OF MILITARY PERSONNEL<br>(EMPLOYEES) OF STRUCTURAL UNITS OF SECURITY AGENCIES<br>Surkov Aleksey, Baranov Andrew .....                                                                       | 56        |
| LEGAL CONSEQUENCES OF PERSONAL DATA BREACHES<br>Tishchenko Irina .....                                                                                                                                                             | 57        |
| COMPARATIVE ANALYSIS OF CRIMINAL LAW PROTECTION<br>FROM COMPUTER CRIMES IN INDIA AND IN RUSSIA<br>Khazinurova Ekaterina .....                                                                                                      | 58        |
| <b>INFORMATION TECHNOLOGY SECURITY .....</b>                                                                                                                                                                                       | <b>60</b> |
| ANOMALY DETECTION IN INFORMATION SYSTEMS BASED ON HETEROGENEOUS<br>GRAPH NEURAL NETWORKS AND LARGE LANGUAGE MODELS<br>Abramenko Georgii, Kotenko Igor .....                                                                        | 60        |
| INFORMATION SECURITY RISK MANAGEMENT IN NATIONAL GUARD UNITS IN THE CONTEXT<br>OF THE DEVELOPMENT AND DISSEMINATION OF ARTIFICIAL INTELLIGENCE<br>Afonin Petr .....                                                                | 62        |
| PREREQUISITES AND PURPOSE OF THE UNINTENTIONAL INSIDER BEHAVIOR MODEL<br>IN THE ORGANIZATION'S INFORMATION SYSTEM<br>Buinevich Mikhail, Moiseenko Grigory, Zhernova Ksenia .....                                                   | 64        |
| USER ACTIVITY ANALYZING ON THE «VKONTAKTE» SOCIAL NETWORK<br>Vitkova Lidia, Lebedeva Daria .....                                                                                                                                   | 65        |
| META-MODEL OF AN ORGANIZATIONAL EMPLOYEE FOR DETECTING INSIDER ACTIVITY<br>Vlasov Dmitry, Meleshko Alexey .....                                                                                                                    | 66        |
| MODELS OF ATTACKS, TRACES, AND INCIDENT ENVIRONMENTS USING FUZZY LOGIC<br>Gorda Maxim, Chechulin Andrey .....                                                                                                                      | 68        |
| ENSURING INFORMATION SECURITY TO IMPROVE ENTERPRISE MANAGEMENT EFFICIENCY<br>Grachev Mikhail .....                                                                                                                                 | 69        |
| AI-ASSISTED SBOM ANALYSIS AND VULNERABILITY TRIAGE IN OPEN-SOURCE SOFTWARE<br>Davydov Vitaly, Kozyrev Vladislav .....                                                                                                              | 70        |
| DEVELOPMENT OF SECURE PROTOCOL FOR DECENTRALIZED MANAGEMENT<br>IN WIRELESS SENSOR NETWORKS<br>Desnitsky Vasily .....                                                                                                               | 72        |
| EVALUATION OF A RESEARCH PROTOTYPE OF A SELF-ORGANIZING DECENTRALIZED<br>WIRELESS SENSOR NETWORK<br>Desnitsky Vasily .....                                                                                                         | 73        |
| ON THE INFLUENCE OF ARCHITECTURAL DECISIONS ON THE SECURITY<br>OF DECISION-MAKING IN INFORMATION AND CONTROL SYSTEMS<br>Dubenetsky Vladislav, Kuznetsov Alexander, Tsekhanovsky Vladislav .....                                    | 74        |
| CHOICE OF THE EXTENSION DEGREE OF A BINARY FIELD FOR DEFINING VECTOR<br>FINITE FIELDS AS SUPPORTS OF PUBLIC-KEY CRYPTALGORITHMS<br>ON HARD-TO-INVERTIBLE MAPPINGS<br>Zakharov Dmitriy, Moldovyan Alexandr, Moldovyan Dmitriy ..... | 76        |
| ANALYSIS OF THE FEDERATED CLUSTERING ALGORITHMS<br>Zabaluev Daniil, Kolpaschikov Maxim .....                                                                                                                                       | 78        |
| FINITE MATRIX ALGEBRAS AS ALGEBRAIC SUPPORTS OF DIGITAL SIGNATURE<br>ALGORITHMS WITH A HIDDEN GROUP<br>Zakharov Dmitriy, Moldovyan Dmitriy, Moldovyan Nikolay .....                                                                | 80        |



|                                                                                                                                                                           |     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| ADVERSARIAL ATTACKS ON THE INPUT DATA OF THE ARTIFICIAL NEURAL RECOGNITION NETWORK: THEORY AND EXPERIMENT<br>Zelentsova Elena, Vitkova Lidia .....                        | 81  |
| DETECTING MULTI-STEP CYBER-ATTACKS IN COMPUTER NETWORKS BASED ON A COMBINATION OF MACHINE LEARNING AND BIG DATA PROCESSING METHODS<br>Zelichenok Igor, Kotenko Igor ..... | 83  |
| INFORMATION SECURITY TOOLS FOR LINUX FAMILY OPERATING SYSTEMS<br>Ivakina Maria, Shilkov Vladimir .....                                                                    | 85  |
| SPATIAL PRIVACY: RISKS, MASKING AND TRUST ARCHITECTURE IN GEO DATA PROCESSING<br>Izotov Daniil, Yarovoy Robert .....                                                      | 87  |
| VULNERABILITIES OF LARGE LANGUAGE MODELS: ATTACK VECTORS AND COMPREHENSIVE COUNTERMEASURES<br>Klishin Alexander, Yarovoy Robert .....                                     | 88  |
| GENERATIVE MODELS AS A TOOL OF SOCIAL ENGINEERING: THREATS AND COUNTERMEASURES<br>Klishin Alexander, Yarovoy Robert .....                                                 | 89  |
| DATA DE-PERSONALISATION IN BIG LANGUAGE MODELS: THE BOUNDARIES OF PRIVACY<br>Klishin Alexander, Yarovoy Robert .....                                                      | 90  |
| AI-BASED APPROACHES TO ANOMALY DETECTION IN WEB TRAFFIC<br>Kolinko Inna .....                                                                                             | 91  |
| A METHOD FOR INCREASING THE PERFORMANCE OF ALGEBRAIC SIGNATURE ALGORITHMS WITH A HIDDEN GROUP<br>Kostina Anna .....                                                       | 93  |
| METHODOLOGY FOR INCREASING THE SECURITY OF THE DISTRIBUTED LEDGER OF SMART CITY SYSTEMS<br>Krundyshev Vasiliy, Kalinin Maxim .....                                        | 94  |
| REDUCING THE PROBLEM OF DESIGNING GRAPHIC INTERFACES TO OPTIMIZATION<br>Kurt Pavel, Izrailov Konstantin .....                                                             | 96  |
| ARCHITECTURE OF A SYSTEM FOR PROTECTION OF SOLUTIONS BASED ON LARGE LANGUAGE MODELS FOR INTERNET OF THINGS DEVICES<br>Lavrentiev Vladimir, Levshun Dmitry .....           | 97  |
| SOFTWARE SECURITY PROBLEMS FROM THE POSITION OF SYSTEM ANALYSIS<br>Leonov Nikolay, Buinevich Mikhail, Antonyuk Yevgeniy .....                                             | 99  |
| INFORMATION SECURITY: THE ROLE OF REQUIREMENTS AND ARCHITECTURE OF THE INFORMATION SYSTEM<br>Litvinov Evgeniy, Ananeva Varvara .....                                      | 100 |
| COMPREHENSIVE ASPECTS OF MOBILE DEVICE SECURITY: THREATS, VULNERABILITIES, PROTECTION<br>Lukashenok Vasily, Yarovoy Robert .....                                          | 102 |
| CREATION OF A DATA SET FOR WATER TREATMENT SECURITY TASKS<br>Meleshko Aleksei .....                                                                                       | 103 |
| ANOMALIES DETECTION IN CONTAINER SYSTEMS BASED ON SECURITY PARAMETER PROFILING<br>Melnik Maxim, Kotenko Igor .....                                                        | 104 |

|                                                                                                                                                                                     |     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| METHODS FOR ENHANCED RANDOMIZATION IN ALGEBRAIC HIDDEN GROUP<br>DIGITAL SIGNATURE ALGORITHMS<br>Morozova Elena, Kostina Anna .....                                                  | 106 |
| A NEW TYPE OF POST-QUANTUM SIGNATURE SCHEMES ON FINITE MATRIX ALGEBRAS<br>Morozova Elena, Mikhachenko Alexandra, Moldovyan Nikolay .....                                            | 108 |
| BALANCED ALGEBRAIC SIGNATURE ALGORITHMS BASED ON THE COMPUTATIONAL<br>HARDNESS OF SOLVING LARGE SYSTEMS OF EQUATIONS<br>Morozova Elena, Shcherbacov Victor, Moldovyan Nikolay ..... | 109 |
| APPLICATION OF ONTOLOGICAL MODELING FOR RISK MANAGEMENT<br>IN INDUSTRIAL CYBER-PHYSICAL SYSTEMS SECURITY<br>Novikova Evgenia, Meleshko Aleksei .....                                | 111 |
| MINIMUM SECURITY REQUIREMENTS FOR BIG DATA PROCESSING<br>AND STORAGE SYSTEMS<br>Poltavtseva Maria, Aleksandrova Elena, Voroshin Evgenii .....                                       | 113 |
| DATABASE SECURITY METHODS<br>Puchkov Vladimir, Vitkova Lidia .....                                                                                                                  | 115 |
| ETHICAL HACKING IN CYBERSECURITY STRATEGY<br>Ryabov Gennady, Yarovoy Robert .....                                                                                                   | 116 |
| ANALYSIS OF THE USE OF AUTOENCODERS TO IMPROVE ACCURACY<br>IMAGE CLASSIFICATIONS<br>Sadovnikov Vladimir, Saenko Igor .....                                                          | 117 |
| MAIN CHARACTERISTICS AND SELECTION OF SECURED OPERATING SYSTEMS<br>FOR CRITICAL INFRASTRUCTURE<br>Seller Anastasiia .....                                                           | 118 |
| INFORMATION SECURITY THREATS AND VULNERABILITIES<br>IN DISTRIBUTED CLOUD ARCHITECTURES<br>Senin Oleg, Yarovoy Robert .....                                                          | 120 |
| THREATS AND SECURITY IN CONTAINERIZATION INFRASTRUCTURE:<br>ANALYSIS OF SECURITY APPROACHES AND PRACTICES<br>Senin Oleg, Yarovoy Robert .....                                       | 121 |
| LLM AS A TOOL FOR DETECTING AND FORECASTING CYBER THREATS<br>Senin Oleg, Yarovoy Robert .....                                                                                       | 122 |
| LLM AS AN INTELLIGENT TOOL FOR REVERSE ENGINEERING OF MALWARE<br>Senin Oleg, Yarovoy Robert .....                                                                                   | 123 |
| LLM IN INFORMATION SECURITY: PRACTICAL SCENARIOS, VULNERABILITIES<br>AND APPLICABILITY LIMITS<br>Senin Oleg, Yarovoy Robert .....                                                   | 124 |
| DETECTION OF VULNERABILITIES IN INFORMATION AND COMPUTING NETWORKS<br>BASED ON REINFORCED LEARNING<br>Maksim Sletov, Kotenko Igor .....                                             | 125 |
| DETECTING ATTACKS ON WEB APPLICATIONS USING A COMBINED<br>MLP-BASED APPROACH<br>Sobolev Pavel, Kotenko Igor .....                                                                   | 126 |
| THE EVOLUTION OF PHISHING: FROM MASS MAILINGS TO AUTONOMOUS AI AGENTS<br>Stakhov Maxim .....                                                                                        | 127 |
| APPROACHES TO ENSURING THE SECURITY OF CROSS-CHAIN INTERACTIONS<br>Terovec Aleksei, Kushnir Dmitry .....                                                                            | 131 |

|                                                                                                                                                                                                                                                 |            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| ENSURING DATA INTEGRITY IN LOCAL NETWORKS BASED ON BLOCKCHAIN TECHNOLOGIES<br>Shevyakov Vladislav, Saenko Igor .....                                                                                                                            | 133        |
| ANALYTICS OF REPLACEABILITY OF OPERATING SYSTEMS IN INFORMATIZATION<br>OF DISCIPLINES OF THE EDUCATIONAL PROCESS<br>Shirokov Vladimir, Schigoleva Marina .....                                                                                  | 134        |
| RECONSTRUCTION OF A CRYPTOGRAPHIC KEY FROM AN IRIS IMAGE<br>USING A NEURAL NETWORK MODEL<br>Shtuka Stanislav, Borshevnikov Aleksey .....                                                                                                        | 136        |
| PRINCIPLES OF BUILDING FAULT-RESISTANT AND PROTECTED GIS ARCHITECTURES<br>TO SUPPORT ADAPTIVE DESIGN SOLUTIONS IN THE EMERCOM OF RUSSIA<br>Gryzunov Vitaly, Sagitov Azat.....                                                                   | 137        |
| <b>INFORMATION SECURITY OF TELECOMMUNICATION NETWORKS.....</b>                                                                                                                                                                                  | <b>139</b> |
| DIRECTIONS OF AUTOMATION OF INFORMATION PROTECTION IN INFORMATION<br>AND COMMUNICATION SYSTEMS<br>Avramenko Vladimir .....                                                                                                                      | 139        |
| SOFTWARE COMPLEX FOR DETERMINING THE LOCATION OF INTERNAL SECURITY<br>VIOLATIONS IN COMPUTER NETWORKS<br>Avramenko Vladimir .....                                                                                                               | 140        |
| FORECASTING THE PROTECTION OF INFORMATION IN AUTOMATED SYSTEMS<br>Avramenko Vladimir, Orlov Aleksei.....                                                                                                                                        | 141        |
| GEOCONTROLLING: APPROACHES TO THE IMPLEMENTATION OF SUPPORT<br>FOR THE MANAGEMENT OF TERRITORIAL ACTIVITY<br>Zvezdarev Dmitry, Efremov Dmitry, Bidenko Sergey, Belyaev Alexander.....                                                           | 143        |
| FUNCTIONING FEATURES AND CONDITIONS OF USE OF TRUSTED LOADING TOOLS<br>OF THE BASIC INPUT-OUTPUT SYSTEM LEVEL AT AUTOMATED WORKPLACES<br>OF USERS OF TELECOMMUNICATION NETWORKS AND TECHNOLOGIES<br>Vinogradov Vladislav, Parashchuk Igor ..... | 146        |
| MODELING THE STATE OF THE EXTERNAL ENVIRONMENT WITH IDENTIFICATION<br>OF TERRITORIES OF DANGEROUS ATMOSPHERIC AND TECHNOGENIC IMPACTS<br>Glushchenko Artem .....                                                                                | 148        |
| GENERATIVE APPROACH TO CREATING ANONYMIZED DIGITAL TWINS<br>OF TELECOMMUNICATION BUSINESS PROCESSES IN THE FORMAT<br>OF A KNOWLEDGE GRAPH<br>Golovin Aleksei, Zhukova Nataly .....                                                              | 149        |
| A MODERN APPROACH TO CONSTRUCTING SOFTWARE-DEFINED<br>WIRELESS COMMUNICATION NETWORKS<br>Gordeev Mikhail, Olimpiev Aleksey .....                                                                                                                | 151        |
| APPLICATION OF QUANTUM TECHNOLOGIES IN DATA CENTERS<br>Gribkov Vladimir, Mikhailichenko Nikolay, Titov Vladimir, Sharko Gennady .....                                                                                                           | 152        |
| FEATURES OF THE FUNCTIONING OF THE Internet OF THINGS IN DATA CENTERS<br>Gribkov Vladimir, Mikhailichenko Nikolay, Titov Vladimir, Sharko Gennady .....                                                                                         | 154        |
| ENSURING THE RESILIENCE OF A BLOCKCHAIN-ENABLED SYSTEM TO SECURITY THREATS<br>BASED ON AN INTEGRATED COMPLEX OF PROTECTION AND VERIFICATION METHODS<br>Kalinin Maxim, Bushmelev Artem.....                                                      | 157        |
| MODELING OF INFORMATION SECURITY IN AN INFORMATION SYSTEM<br>USING INNOVATIVE TECHNOLOGIES<br>Karganov Vitaly .....                                                                                                                             | 159        |

|                                                                                                                                                                                                                                                                             |     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| INFORMATION-THEORETICAL ANALYSIS OF COMMUNICATION CHANNELS:<br>SECURITY METRICS AND APPLICABILITY LIMITS<br>Klishin Alexander, Yarovoy Robert .....                                                                                                                         | 161 |
| DDOS ATTACKS ON TELECOMMUNICATIONS: VULNERABILITIES AND DEFENSE STRATEGY<br>Klishin Alexander, Yarovoy Robert .....                                                                                                                                                         | 162 |
| SOME ASPECTS OF THE NEED FOR SPECIAL PURPOSE SYSTEM MODELING<br>Kovalev Igor, Pantyukhin Oleg, Loginov Vyatcheslav, Nogin Sergey .....                                                                                                                                      | 163 |
| ASSESSMENT OF CRITICAL INFRASTRUCTURE SECURITY: GENERAL ISSUES<br>AND DETAILING OF THE GOALS AND OBJECTS OF INFORMATION SECURITY<br>AUDIT USING THE EXAMPLE OF A WATER TREATMENT SYSTEM<br>Kotenko Igor, Saenko Igor, Parashchuk Igor .....                                 | 165 |
| USER ACCESS TO ELECTRONIC EDUCATIONAL RESOURCES AND ELECTRONIC DIDACTIC<br>INFORMATION VIA PUBLIC COMMUNICATION CHANNELS:NATURE,<br>OBJECTIVES AND CRITERIA OF SECURITY AUDIT<br>Kryukova Elena, Parashchuk Igor .....                                                      | 167 |
| THE USE OF GSM MOBILE BASE STATIONS IN MODERN<br>COMMUNICATION AND SECURITY SYSTEMS<br>Kuzoyatov Vladislav, Iudin Anatolii .....                                                                                                                                            | 169 |
| PROBLEM OF DEFENSE AGAINST MULTI-STEP SOCIAL ENGINEERING ATTACKS.<br>ANALYSIS OF THE MAIN ELEMENTS<br>Kyuner Andrey, Chechulin Andrey .....                                                                                                                                 | 171 |
| ACCELERATING THE TACTILE INTERNET WITH THE QUICK UDP INTERNET CONNECTIONS<br>TRANSPORT PROTOCOL: SECURITY AND PRIVACY PERSPECTIVE<br>Lauta Oleg, Mitrofanov Mikhail .....                                                                                                   | 173 |
| ON THE QUESTION OF CONSTRUCTING DIGITAL TWINS AND RAPID PROTOTYPING<br>OF ALGORITHMS AND SOFTWARE FOR INSURSION DETECTION SYSTEMS<br>Levshun Dmitry, Kotenko Igor, Parashchuk Igor .....                                                                                    | 174 |
| TO THE QUESTION OF MULTICRITERIAL ANALYSIS OF INFORMATION SECURITY<br>OF NETWORKS AND FACILITIES BASED ON THE INTERNET OF THINGS<br>TECHNOLOGY AT CRITICAL INFRASTRUCTURE FACILITIES<br>Levshun Dmitry, Parashchuk Igor .....                                               | 176 |
| IMPLEMENTATION OF CYBERSECURITY MANAGEMENT OF A DATA TRANSMISSION<br>NETWORK USING MACHINE LEARNING-BASED DECISION SUPPORT TOOLS<br>Lipatnikov Valery, Shevchenko Alexander, Melekhov Kirill .....                                                                          | 179 |
| ANALYSIS OF SECURITY AND MAINTENANCE INDICATORS OF DATA CENTERS AS OBJECTS<br>OF CRITICAL INFOCOMMUNICATION INFRASTRUCTURE USING AN ONTOLOGICAL<br>APPROACH AND METHODS OF INTELLIGENT DATA ANALYSIS<br>Mikhailichenko Anton, Mikhailichenko Nikolay, Parashchuk Igor ..... | 180 |
| SECURITY OF MACHINE-TO-MACHINE INFORMATION EXCHANGE BETWEEN DATA CENTERS:<br>AN APPROACH TO GROUPING THREAT SIGNS AND TYPOLOGIZING RISKS<br>Mikhailichenko Nikolay, Parashchuk Igor .....                                                                                   | 182 |
| ANALYSIS OF THE SECURITY OF MOBILE APPLICATIONS FOR SECURE DATA TRANSMISSION<br>Nikolaeva Polina .....                                                                                                                                                                      | 184 |
| ANALYSIS OF THE SECURITY OF CLOUD SERVICES AND DATA PROTECTION METHODS<br>Nikolaeva Polina .....                                                                                                                                                                            | 185 |
| PROTECTION OF VOICE COMMUNICATION CHANNELS FROM DEEPFAKE ATTACKS<br>Nikolaeva Polina .....                                                                                                                                                                                  | 186 |
| MONITORING IDENTIFICATION METHODS FOR ABNORMAL TRAFFIC ON THE NETWORK<br>Nogin Syrgey, Sychev Kirill, Emilianenko Artur .....                                                                                                                                               | 187 |

|                                                                                                                                                                                                                                          |     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| ABOUT MONITORING THE LOCAL NETWORK<br>Nogin Syrgey, Sychev Kirill, Emelianenko Artur .....                                                                                                                                               | 189 |
| INFORMATION SECURITY AND INFORMATION PROTECTION IN THE CONTEXT<br>OF DEVELOPMENT OF DIGITAL TELECOMMUNICATIONS<br>AND MACVIL TECHNOLOGY<br>Nuralinov Azamat, Malikbayev Talgat.....                                                      | 191 |
| SOME ASPECTS OF SAFE DATA SEARCH ON THE RESOURCES OF A UNIFIED SYSTEM<br>OF DATA CENTERS AND CLOUD STORAGE AS A KEY ELEMENT<br>OF INFORMATION SUPPORT FOR OFFICIALS<br>Osadchiy Alexander, Popkov Yuri, Nosov Mikhail .....              | 192 |
| MONITORING THE PERFORMANCE OF IP TELEPHONY NETWORKS AND EVALUATING<br>THE QUALITY OF SERVICES PROVIDED USING A SOFTWARE MODULE<br>IN THE CONTEXT OF CYBERATTACKS<br>Privolov Andrey, Titov Daniil, Bobotina Polina .....                 | 194 |
| PROMISING AREAS OF EFFICIENCY IMPROVEMENT DATA PROCESSING<br>Renskov Andrey, Renskov Dmitry .....                                                                                                                                        | 196 |
| THE USE OF MODERN CYBERSECURITY TECHNOLOGIES AND METHODS<br>TO PROTECT REGIONAL INFORMATION SYSTEMS<br>Renskov Dmitry.....                                                                                                               | 198 |
| TASKS, STAGES AND METHODS OF ENSURING SECURITY ANALYSIS OF DEPARTMENTAL<br>TELECOMMUNICATION NETWORKS OF CRITICAL FACILITIES WHEN<br>THEY WORK WITH A PUBLIC NETWORK<br>Ryabov Gennady, Parashchuk Igor .....                            | 201 |
| ANALYSIS OF GENERAL AND SPECIFIC REQUIREMENTS TO THE SYSTEM FOR DETECTING<br>MALICIOUS ACTIVITIES IN THE TRAFFIC OF NFOCOMMUNICATION NETWORKS<br>AND SYSTEMS OF INDUSTRIAL SMART CITY<br>Saenko Igor, Kotenko Igor, Parashchuk Igor..... | 203 |
| AN OPTION FOR IMPROVING THE STEALTH OF INFORMATION<br>BASED ON CHANGING CHAOTIC CARRIER SIGNALS<br>Sazonov Viktor, Albadr Khodr .....                                                                                                    | 205 |
| INTERFACES FOR IMPLEMENTING SEARCH QUERY: FORMULATION AND JUSTIFICATION<br>OF SECURITY ASSESSMENT METRICS AND SUBMETRICS<br>Sayarkin Leonid, Parashchuk Igor, Seleznev Andrey .....                                                      | 206 |
| ENSURING THE INFORMATION SECURITY OF THE LORA WIRELESS<br>DATA TRANSMISSION NETWORK<br>Silchev Kirill.....                                                                                                                               | 208 |
| DEEP LEARNING FOR ANOMALIES DETECTION IN NETWORK TRAFFIC<br>Sitdikov Dmitry, Leshchinsky Bogdan, Shevchenko Alexander.....                                                                                                               | 210 |
| ARTIFICIAL INTELLIGENCE FOR SECURING INTERNET OF THINGS COMMUNICATIONS<br>Sitdikov Dmitry, Leshchinsky Bogdan, Shevchenko Alexander .....                                                                                                | 211 |
| EXPLAINABLE ARTIFICIAL INTELLIGENCE IN TELECOMMUNICATION NETWORK<br>INTRUSION DETECTION SYSTEMS<br>Sitdikov Dmitry, Leshchinsky Bogdan, Shevchenko Alexander .....                                                                       | 213 |
| TRUST PRACTICES FOR ML MODELS: SHA-256 INTEGRITY CONTROL AND BEHAVIORAL<br>PARITY OF PYTORCH AND TENSORFLOW AFTER DESERIALIZATION<br>Sitdikov Dmitry, Leshchinsky Bogdan, Shevchenko Alexander .....                                     | 214 |
| INTRUSION DETECTION SYSTEMS IN PROGRAM-DEFINED NETWORKS: ANALYSIS<br>OF MODERN SOLUTIONS, THREATS, AND PROTECTION METHODS<br>Starodubtsev Yuri, Mitrofanov Mikhail.....                                                                  | 215 |

|                                                                                                                                                                                                                                     |            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| INTERVAL ASSESSMENT OF THE QUALITY OF MANAGERIAL, METHODOLOGICAL<br>AND PRACTICAL SKILLS OF OFFICIALS OF INFORMATION SECURITY BODIES<br>OF TELECOMMUNICATION NETWORKS<br>Shamiev Vyacheslav, Pantyukhin Oleg, Parashchuk Igor ..... | 217        |
| DEVELOPMENT OF AN ANALYTICAL APPARATUS FOR DECISION SUPPORT SYSTEMS<br>IN PLANNING DATA TRANSMISSION NETWORKS<br>Sharko Gennady, Sharko Tamara .....                                                                                | 219        |
| <b>INFORMATION AND ECONOMIC SECURITY .....</b>                                                                                                                                                                                      | <b>221</b> |
| THE IMPACT OF SOFTWARE IMPORT SUBSTITUTION ON THE LEVEL OF INFORMATION<br>AND ECONOMIC SECURITY OF INDUSTRIAL ENTERPRISES<br>Aminov Khakimdzhon, Leskova Elizaveta .....                                                            | 221        |
| INFORMATION AND ECONOMIC SECURITY OF THE AGRO-INDUSTRIAL COMPLEX<br>IN THE CONTEXT OF DIGITAL TRANSFORMATION ON THE EXAMPLE<br>OF THE KRASNODAR TERRITORY APPLICATION<br>Aminov Khakimdzhon, Semikolennykh Vladimir .....           | 223        |
| THE IMPACT OF CYBERSECURITY MEASURES ON THE ECONOMIC STABILITY<br>OF A COMPANY<br>Andreevskiy Igor, Kuznetsova Olga .....                                                                                                           | 224        |
| INFORMATION SECURITY THREATS WHEN BUILDING A CORPORATE CLOUD<br>ANALYTICAL SOLUTION<br>Bobchinskiy Artem, Andreevskiy Igor .....                                                                                                    | 226        |
| INFORMATION SECURITY OF BIG DATA IN THE TASKS OF ECONOMICS<br>AND MANAGEMENT<br>Anikin Yury, Shilkov Vladimir, Ivakina Maria .....                                                                                                  | 228        |
| DIGITAL TRANSFORMATION OF WATER SUPPLY SYSTEMS AND CYBERSECURITY<br>Anikin Yury, Shilkov Vladimir .....                                                                                                                             | 230        |
| FROM INVENTORY TO CYBER-PROTECTION: PRACTICAL APPLICATION OF IT-ASSET<br>MANAGEMENT PRACTICES IN THE INFORMATION SECURITY CONTEXT<br>Vasilisin Pavel .....                                                                          | 233        |
| CORPORATE APPROACH TO THE ORGANIZATION OF MULTIPLE ACCESS<br>TO INFORMATION AND COMMUNICATION RESOURCES<br>Verzun Natalia, Kolbanev Mikhail, Konturov Andrey .....                                                                  | 234        |
| SOME ASPECTS OF INFORMATION AND ECONOMIC SECURITY<br>IN TERMINAL ACCESS TECHNOLOGIES<br>Emelyanov Alexandr, Peskova Elizaveta .....                                                                                                 | 235        |
| TRANSPORT AND LOGISTICS SYSTEM OF THE OVERPASS TYPE UST AS A STRATEGIC<br>SOLUTION FOR THE ARCTIC: ENGINEERING AND SOCIO-ECONOMIC ASPECT<br>Erofeevskii Daniil, Mitko Arseniy .....                                                 | 237        |
| CYBERSECURITY ECONOMICS IS ONE OF THE PRIORITIES<br>OF DIGITAL TRANSFORMATION FOR ENTERPRISES<br>Korshunov Igor, Mikadze Sergey, Solovyova Yanita .....                                                                             | 239        |
| RISKS OF USING ARTIFICIAL INTELLIGENCE IN THE ECONOMY<br>Igor Korshunov, Vladimir Tumarev, Alina Shumaeva .....                                                                                                                     | 241        |
| MODEL OF DIGITAL TRANSFORMATION OF AGRICULTURE<br>Maslov Nikita .....                                                                                                                                                               | 244        |
| MATHEMATICAL MODEL OF AN ACOUSTIC FAULT RECOGNITION SYSTEM<br>FOR TECHNICAL OBJECTS<br>Verzun Natalia, Kolbanev Mikhail, Salieva Adelina .....                                                                                      | 245        |

|                                                                                                                                                                         |            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| DEVELOPMENT AND EXPERIMENTAL STUDY OF THE TRAINING METHOD<br>WITH REINFORCEMENT FOR THE TASKS OF ACOUSTIC DIAGNOSIS<br>OF INDUSTRIAL EQUIPMENT<br>Salieva Adelina ..... | 247        |
| <b>INFORMATION SECURITY OF TRANSPORT SYSTEMS .....</b>                                                                                                                  | <b>249</b> |
| EVOLUTION OF MARINE PROPULSION SYSTEMS<br>Amelakhanov Daniil, Zhuravlev Anton .....                                                                                     | 249        |
| USING TELEMATICS IN TRANSPORT<br>Bogdanova Polina .....                                                                                                                 | 251        |
| ALGORITHM FOR DISTANCE MANAGEMENT OF MEETING VESSELS BASED<br>ON THE METHOD OF POTENTIAL FIELDS<br>Danilin German, Khudainazarov Yuri, Sokolov Sergey .....             | 253        |
| EVALUATION OF THE PERFORMANCE OF AUTOMOTIVE LIDAR AND RADAR SYSTEMS<br>IN BAD VISIBILITY CONDITIONS<br>Vavkina Elena .....                                              | 254        |
| METHODOLOGY FOR ASSESSING THE ACCESSIBILITY OF A CORPORATE COMMUNICATION<br>SYSTEM TO RADIO CONTROL AND TECHNICAL COMPUTER CONTROL<br>Efanov Anton, Ivanov Sergey ..... | 256        |
| MACHINE VISION IN AUTONOMOUS VEHICLE SYSTEMS THREAT<br>AND TRUST ARCHITECTURES<br>Izotov Daniil, Yarovoy Robert .....                                                   | 258        |
| INFORMATION SECURITY IS A KEY ELEMENT IN ENSURING THE VIABILITY<br>OF SUPPLY CHAINS<br>Iskanderov Yury .....                                                            | 259        |
| INTELLIGENT SYSTEM FOR INFORMATION SECURITY MANAGEMENT<br>OF TRANSPORT AND LOGISTICS PROCESSES<br>Iskanderov Yury .....                                                 | 261        |
| MACHINE LEARNING METHODS FOR PROTECTING COMMUNICATION CHANNELS<br>IN INTELLIGENT TRANSPORT SYSTEMS<br>Kalekina Maria, Nyrkov Anatoly .....                              | 263        |
| ANALYSIS OF TOOLS FOR IMPROVING THE PRODUCTIVITY OF PORT WORKFLOWS<br>Kubovskii Artemy, Zhuravlev Anton .....                                                           | 264        |
| ABOUT INFORMATION SECURITY OF UNMANNED WATER TRANSPORT<br>Nyrkov Anatoliy, Khudainazarov Yuri .....                                                                     | 266        |
| DEVSECOPS APPROACH TO DEVELOPING SOFTWARE FOR AUTONOMOUS<br>TRANSPORT SYSTEMS<br>Prokopenko Daniil .....                                                                | 268        |
| QUANTUM CRYPTOGRAPHY IN UNMANNED SYSTEMS:<br>CHALLENGES AND EVALUATION CRITERIA<br>Rybakova Taisiia .....                                                               | 269        |
| FUNCTIONAL MONITORING OF UNMANNED VEHICLES UNDER EXTERNAL IMPACTS<br>Semenov Viktor .....                                                                               | 271        |
| ENHANCED VIABILITY OF THE SEAPORT MANAGEMENT SYSTEM<br>Khasanov Dmitry .....                                                                                            | 272        |
| AUTOMATION OF PENETRATION TESTING PROCESSES: OPPORTUNITIES,<br>LIMITATIONS AND DEVELOPMENT<br>Yumasheva Elena .....                                                     | 275        |

|                                                                                                                                                                                                                                          |            |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>INFORMATION SECURITY OF MARINE EQUIPMENT AND MARINE INFRASTRUCTURE .....</b>                                                                                                                                                          | <b>277</b> |
| INTELLECTUALIZATION OF DECISION-MAKING SUPPORT FOR DIGITAL TWIN TECHNOLOGY<br>OF SYSTEMS FIGHTING FOR THE INFORMATION SURVIVABILITY OF A SHIP, VESSEL<br>Mikhailchuk Andrey, Alekseev Anatoly, Antipov Vasily, Smolnikov Alexander ..... | 277        |
| DIGITALIZATION OF THE QUALITY OF COMPREHENSIVE INFORMATION PROTECTION<br>IN THE CERTIFICATION OF INNOVATIVE SOLUTIONS<br>Alekseev Anatoly .....                                                                                          | 279        |
| INFORMATIONAL SURVIVABILITY OF A SHIP: A MASTER CLASS<br>Alekseev Anatoly .....                                                                                                                                                          | 281        |
| ON THE ISSUE OF DEVELOPING A SYSTEM FOR EFFECTIVE AND OBJECTIVE<br>RANKING OF INFORMATION SECURITY TOOLS<br>Bogatyrev Danil.....                                                                                                         | 283        |
| ENSURING CYBERSECURITY OF INDUSTRIAL CONTROL SYSTEMS<br>Varenitsa Lidia .....                                                                                                                                                            | 284        |
| INTEGRATION OF CNC TECHNOLOGIES INTO THE DIGITAL ECOSYSTEM<br>OF SHIPBUILDING IN A SECURE DESIGN<br>Vasyukova Maria.....                                                                                                                 | 286        |
| ON THE PRACTICAL DEVELOPMENT OF A CAD SYSTEM AT THE SHIP REPAIR<br>CENTER OF JSC «CS» «ZVEZDOCHKA», USING QUALITY RANKING<br>IN A PROTECTED EXECUTION<br>Vereshchagin Anatoly .....                                                      | 287        |
| EVALUATION OF THE USE OF PKK-KASOR 23.5 IN THE FIELD OF PROTECTION<br>OF MARINE INFRASTRUCTURE FACILITIES IN A SECURE DESIGN<br>Vcherashniy Mikhail .....                                                                                | 289        |
| DIGITAL ASSESSMENT OF THE INTEGRATED INFORMATION PROTECTION<br>OF A DISTRIBUTED FLOTILLA MANAGEMENT SYSTEM OF DIVERSE FORCES<br>Drigola Vladimir, Alekseev Anatoly .....                                                                 | 290        |
| INFORMATION STEALTH OF A HYBRID POWER PLANT FOR UNMANNED SURFACE VESSELS<br>Evdokimov Nikita.....                                                                                                                                        | 292        |
| MODELING AND FORECASTING SHIP FUEL CONSUMPTION<br>USING MACHINE LEARNING METHODS<br>Erofeevskii Daniil, Mitko Arseniy.....                                                                                                               | 293        |
| THE INTRODUCTION OF MDM PLATFORMS INTO THE DIGITAL PROCESSES<br>OF THE SHIPBUILDING INDUSTRY AS AN ELEMENT OF SECURE<br>DIGITAL TRANSFORMATION<br>Zinovev Arthur .....                                                                   | 295        |
| INFORMATION SECURITY SUBSYSTEM FOR INTELLIGENT SUPPOR<br>OF TRANSPORTATION OF OVERSIZED CARGO<br>Iliukhin Petr .....                                                                                                                     | 296        |
| UPDATING THE DATABASE AND KNOWLEDGE OF INFORMATION TECHNOLOGIES<br>OF THE CAM CLASS, TAKING INTO ACCOUNT THE REQUIREMENTS<br>OF INFORMATION SECURITY<br>Kutikova Alevtina, Alekseev Anatoly .....                                        | 297        |
| QUANTITATIVE ASSESSMENT OF ENVIRONMENTAL SAFETY AND DATA PROTECTION<br>USING THE EXAMPLE OF ALMAZ CENTRAL DESIGN BUREAU JSC<br>Lihacheva Elizaveta.....                                                                                  | 298        |
| PROTECTION AGAINST DDoS ATTACKS IN CRITICAL INFRASTRUCTURE<br>Lototskaya Olga.....                                                                                                                                                       | 300        |



|                                                                                                                                                                                                         |            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| A DIGITALIZATION MODEL OF CONTROLLED PRODUCTION PROCESS MANAGEMENT<br>WITH A FEEDBACK LOOP FOR SYSTEM INDICATORS<br>Miklush Sergey .....                                                                | 301        |
| ON THE ISSUE OF PRACTICAL DEVELOPMENT OF SECURE CPC SYSTEMS<br>IN JSC «SPO «ARCTIC» USING QUALIMETRIC RANKING<br>Minichkin Anton .....                                                                  | 303        |
| METHODS FOR ENSURING INFORMATION SECURITY<br>IN WIRELESS SELF-ORGANIZING NETWORKS<br>Minkinen Artemiy .....                                                                                             | 304        |
| DEVELOPMENT OF ENVIRONMENTALLY FRIENDLY MARINE ENGINES POWERED<br>BY ALTERNATIVE FUELS IN A PROTECTED DESIGN<br>Mikhailov Vladimir .....                                                                | 305        |
| ON THE ISSUE OF DEVELOPING AN INTELLIGENT CONTROL SYSTEM<br>FOR UNMANNED VESSELS IN A SECURE DESIGN<br>Nikolaev Denis .....                                                                             | 306        |
| ANALYSIS OF APPROACHES TO THE JOINT OPERATION OF UNMANNED PLATFORMS<br>IN A SECURE DESIGN FOR SEARCH AND RESCUE AND LOGISTICS OPERATIONS<br>IN THE ARCTIC<br>Polezhaev Alexander .....                  | 307        |
| METHODS OF OPTIMIZATION OF MANAGEMENT OF SCIENTIFIC AND PRODUCTION<br>ASSOCIATION IN CONDITIONS OF UNCERTAINTY<br>Ryabkov Yakov, Alekseev Sergey, Artemov Stanislav .....                               | 308        |
| METHODOLOGY AND TECHNOLOGIES OF PROACTIVE MANAGEMENT OF MODERNIZATION<br>OF DISASTER-RESISTANT INFORMATION SYSTEMS<br>IN A SECURE DESIGN<br>Savchenko Maxim .....                                       | 310        |
| ON THE ISSUE OF DEVELOPING A COMPREHENSIVE AUTOMATED SYSTEM<br>FOR MONITORING AND FORECASTING THE TECHNICAL CONDITION<br>OF SHIPBOARD EQUIPMENT IN A SECURE DESIGN<br>Smirnov Petr, Petrov Valery ..... | 312        |
| QUALIMETRIC ASSESSMENT OF ARTIFICIAL INTELLIGENCE-BASED DECISION<br>SUPPORT SYSTEMS FOR OPTIMIZING SECURE MANAGEMENT OF MARINE<br>INFRASTRUCTURE FACILITIES<br>Smorodin Roman .....                     | 313        |
| ON THE ISSUE OF IMPORT SUBSTITUTION IN THE FIELD OF INFORMATION<br>SECURITY OF REGIONS<br>Sokolov Denis .....                                                                                           | 315        |
| ON THE DEVELOPMENT OF AN INTELLIGENT LOGISTICS MANAGEMENT SYSTEM<br>FOR SHIPBUILDING ENTERPRISES IN A SECURE DESIGN<br>Tuzov Alexander .....                                                            | 316        |
| DEVELOPMENT OF A SECURE MACHINE VISION SYSTEM TO PREVENT<br>COLLISIONS OF AUTONOMOUS VESSELS<br>Chavdar Galina .....                                                                                    | 317        |
| <b>INFORMATION AND PSYCHOLOGICAL SECURITY .....</b>                                                                                                                                                     | <b>318</b> |
| INFORMATION AND PSYCHOLOGICAL RISKS OF ARTIFICIAL INTELLIGENCE TOOLS<br>Atysheva Rosa, Shilkov Vladimir .....                                                                                           | 318        |
| EXPANDING THE BOUNDARIES OF UNDERSTANDING CRITICAL THINKING<br>IN THE CONTEXT OF DIGITALIZATION OF SOCIETY AND EDUCATION<br>Baeva Liudmila, Khalifaeva Olga .....                                       | 320        |

|                                                                                                                                                      |            |
|------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| INFORMATION AND PSYCHOLOGICAL SECURITY IN MUSICAL AND CREATIVE<br>ACTIVITIES USING A KEYBOARD SYNTHESIZER<br>Davletova Klara, Romanova Natalia ..... | 321        |
| SOCIOCULTURAL VALUES OF MILITARY JOURNALISM AS AN AXIOLOGICAL<br>INSTRUMENT OF NATIONAL SECURITY<br>Erofeeva Irina, Mikhaleva Lyudmila .....         | 324        |
| COGNITIVE TECHNOLOGIES FOR ENSURING NATIONAL SECURITY OF RUSSIA<br>Kefeli Igor, Kefeli Konstantin .....                                              | 325        |
| SPEECH BEHAVIOR OF THE GERMAN CHANCELLOR: PREFERENCE FOR MENASIVAS<br>Misonzhnikov Boris .....                                                       | 327        |
| COGNITIVE MECHANISMS OF SOCIAL SYSTEMS<br>Plebanek Olga .....                                                                                        | 329        |
| DEVELOPING CRITICAL THINKING IN THE CONTEXT OF DIGITALIZATION OF SOCIETY<br>Khalifaeva Olga .....                                                    | 331        |
| <b>INFORMATION SECURITY IN SOCIOCOMPUTING.....</b>                                                                                                   | <b>333</b> |
| SPREADING RUMORS ON SOCIAL NETWORKS BASED ON THE EXTENDED SCWIEHR MODEL<br>Borisov Sergei .....                                                      | 333        |
| A MODEL OF INFORMATION SECURITY THREATS FOR SOCIAL NETWORK USERS<br>Borisov Sergei .....                                                             | 334        |
| SOCIOCOMPUTING AND AUDIO COMMUNICATIONS: HOW TO PROTECT<br>THE VOICE IN THE DIGITAL ENVIRONMENT<br>Denisova Olga .....                               | 336        |
| LOGISTICS PORTAL CARGOTIME.RU: METHODS OF UNIFICATION<br>OF CONTAINER TRANSPORTATION GEODATA<br>Esin Maxim, Korepanova Anastasya, Sazanov Vadim..... | 337        |
| METAMODELS AND METRICS OF SOCIOCOMPUTING RESILIENCE<br>TO INFORMATION DISTORTIONS<br>Izotov Daniil, Yarovoy Robert .....                             | 339        |
| SCENARIO MODELING OF EXTREME DEVELOPMENT OF INFORMATION<br>ATTACK WAVES IN A DISTURBED SOCIO-INFORMATION SPACE<br>Perevaryukha Andrey .....          | 340        |
| SCENARIO MODELING OF EXTREME DEVELOPMENT OF INFORMATION ATTACK WAVES<br>IN A DISTURBED SOCIO-INFORMATION SPACE<br>Perevaryukha Andrey .....          | 342        |
| <b>INFORMATION SECURITY OF CYBER-PHYSICAL SYSTEMS .....</b>                                                                                          | <b>344</b> |
| ENERGY-EFFICIENT AND SECURE DATA TRANSMISSION SCHEDULING<br>IN KINEMATIC SENSOR NETWORKS<br>Astakhova Tatyana .....                                  | 344        |
| PROOF OF PERSONHOOD IMPLEMENTATION USING NON-TRANSFERABLE TOKENS<br>Bulgakov Dmitry .....                                                            | 346        |
| DICTIONARY ATTACK EFFICIENCY<br>Bulgakov Dmitry .....                                                                                                | 347        |
| REAL-TIME DETECTION OF POTENTIALLY DANGEROUS OBJECTS USING DEEP LEARNING<br>Golovkin Matvey .....                                                    | 349        |

|                                                                                                                                                                                                                                       |            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| DIGITAL TWIN AS A SOURCE OF RISKS: DISCREPANCY WITH REALITY<br>AND THE ARCHITECTURE OF RESILIENCE TO DISCREPANCY<br>Izotov Daniil, Yarovoy Robert .....                                                                               | 350        |
| DIGITAL DOUBLE CYBERSECURITY<br>Krasnova Anna, Lyamin Alexander, Kolbanev Mikhail .....                                                                                                                                               | 351        |
| METHODOLOGY FOR AUTOMATING THE DEVELOPMENT<br>OF ATTACK DETECTION RULES IN SIEM<br>Malakhov Maksim, Vitkova Lidia, Nashivochnikov Nikolay .....                                                                                       | 352        |
| ATTACK AND VIRUS DETECTION BASED ON ARTIFICIAL NEURAL NETWORKS<br>Poymanova Ekaterina .....                                                                                                                                           | 354        |
| OPTIMIZATION OF NEURAL NETWORKS THROUGH SEMI-STRUCTURED<br>SPARSITY OF ACTIVATIONS<br>Raskopina Anastasia .....                                                                                                                       | 356        |
| MIGRATION MODELS IN DATA STORAGE SYSTEMS<br>Reshetnikov Dmitry .....                                                                                                                                                                  | 357        |
| GENERATION OF SYNTHETIC TRAFFIC OF THE INTERNET OF THINGS<br>IN SOLVING INFORMATION SECURITY PROBLEMS<br>Savelyeva Daria .....                                                                                                        | 359        |
| ALGORITHM FOR PROTECTIVE MASKING OF AUDIO INFORMATION<br>USING QUASI-ORTHOGONAL MATRICES<br>Sergeev Mikhail, Sergeev Alexander, Grigoriev Evgeny .....                                                                                | 361        |
| APPLICATION OF NEURAL NETWORK WITH AUTOENCODER ARCHITECTURE<br>TO DETECT NETWORK ATTACKS<br>Tatarnikova Tatiana .....                                                                                                                 | 363        |
| METHODS FOR PREPROCESSING IMAGES OF HANDWRITTEN DOCUMENTS<br>IN COMPUTER VISION TASKS<br>Shikhotov Aleksey .....                                                                                                                      | 364        |
| INTELLECTUAL ANALYSIS OF ROAD TRAFFIC ACCIDENTS<br>IN THE TERRITORY OF TRANSBAIKAL REGION<br>Yurko Artem .....                                                                                                                        | 366        |
| <b>INFORMATION SECURITY OF GEOINFORMATION SYSTEMS.....</b>                                                                                                                                                                            | <b>368</b> |
| INFORMATION SECURITY OF A GEOINFORMATION SYSTEM FOR AI ROUTING<br>OF VESSELS IN ARCTIC WATERS<br>Artamkin Mark, Martyn Irma .....                                                                                                     | 368        |
| INFORMATION SECURITY OF ARCTIC GIS: MACHINE LEARNING FOR NORTHERN<br>SEA ROUTE NAVIGATION SAFETY<br>Bolkhovskiy Ilya .....                                                                                                            | 370        |
| GEOINFORMATION SYSTEM AS AN AUTOMATED CONTROL SYSTEMS BASIS<br>FOR ELECTRIC POWER SYSTEMS OPTIMAL FUNCTIONING UNDER CONDITIONS<br>OF EXTREME WEATHER PHENOMENA IMPACT<br>Burlov Vyacheslav, Polyukhovich Maxim, Logvinova Yulia ..... | 372        |
| GEOINFORMATION SYSTEMS IN THE MANAGEMENT DECISION-MAKING MODEL<br>ARE A SYSTEMATIC APPROACH BASED ON THE LAW OF PRESERVING<br>THE INTEGRITY OF AN OBJECT<br>Grachev Mikhail .....                                                     | 377        |
| A DIRECT AND INVERSE PROBLEM IN THE MANAGEMENT OF GEOGRAPHIC<br>INFORMATION SYSTEMS<br>Grachev Mikhail .....                                                                                                                          | 379        |

|                                                                                                                                                                                                             |            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| PROBLEMS OF GEOINFORMATION SYSTEMS AND METHODS OF THEIR SOLUTION<br>Grachev Mikhail .....                                                                                                                   | 382        |
| A MODEL FOR INTEGRATING GEOSPATIAL DATA INTO OSINT<br>Gryzunov Vitaly .....                                                                                                                                 | 383        |
| VULNERABILITIES IN MACHINE LEARNING MANAGEMENT IN GEOGRAPHIC<br>INFORMATION SYSTEMS<br>Kolbina Olga, Sluzheva Margarita, Mikulyaeva Anastasia .....                                                         | 385        |
| DEVELOPMENT OF ALGORITHMS FOR QUANTUM DATABASES IN INFORMATION SECURITY<br>Kolbina Olga, Fatin Dmitry, Fedoseeva Yana .....                                                                                 | 386        |
| APPLICATION OF DATA SCIENCE TO FORECASTING IN GEOINFORMATION SYSTEMS<br>Kolbina Olga, Grigorieva Olga, Lazareva Vera .....                                                                                  | 387        |
| EDGE COMPUTING FOR IOT-DEVICES<br>Rayan Nabil, Kasumov Gamid .....                                                                                                                                          | 389        |
| VOICE AND GESTURE INTERFACES IN REGIONAL GIS AND CONTROL SYSTEMS:<br>RISKS AND SAFEGUARDS<br>Punkevich Dana, Paymerov Konstantin, Kolbina Olga .....                                                        | 390        |
| THE ROLE OF GEOGRAPHIC INFORMATION SYSTEMS IN ENSURING TRANSPARENCY<br>AND TRUST: CASE STUDIES OF USING OPEN GEODATA FOR POSITIVE<br>REPUTATIONAL POSITIONING<br>Ratushnyak Evgeniy, Gryzunov Vitaliy ..... | 392        |
| <b>TRAINING AND RETRAINING OF STAFF IN INFORMATION SECURITY .....</b>                                                                                                                                       | <b>394</b> |
| THE PROBLEM OF WORKFORCE SHORTAGE IN INFORMATION SECURITY IN RUSSIA:<br>CHALLENGES AND EXPERIENCE OF PRACTICE-ORIENTED SPECIALIST TRAINING<br>Akhrameeva Kseniia .....                                      | 394        |
| DIGITAL LITERACY AS THE BASIS FOR USER INFORMATION SECURITY<br>IN MODERN SOCIETY<br>Borshchenko Viktor .....                                                                                                | 395        |
| PROCESSING DATA FROM UNMANNED AERIAL VEHICLES<br>Grachev Alexander .....                                                                                                                                    | 398        |
| INFORMATION AND PSYCHOLOGICAL SECURITY IN MUSICAL AND CREATIVE<br>ACTIVITIES USING A KEYBOARD SYNTHESIZER<br>Davletova Klara, Romanova Natalia .....                                                        | 400        |
| INTEGRATION OF SOUND DESIGN IN TO EDUCATIONAL PROGRAMS:<br>COLLECTIVE DIGITAL CREATIVE WORK AND SOCIO COMPUTING<br>Deltsova Natalia .....                                                                   | 403        |
| ENSURING INFORMATION SECURITY IN MUSIC EDUCATION<br>Denisova Olga .....                                                                                                                                     | 405        |
| GENERATION OF TRAINING MATERIALS IN THE FIELD OF INFORMATION<br>SECURITY USING LANGUAGE MODELS<br>Karganov Vitaly, Yarovoy Robert .....                                                                     | 406        |
| DEVELOPMENT OF THE COURSE «RECOGNITION TECHNIQUES AND MEASURES TO<br>PROTECT AGAINST TELEPHONE FRAUD» FOR RETRAINING PERSONNEL<br>IN EDUCATIONAL INSTITUTIONS<br>Kovganko Valeria .....                     | 407        |
| AUTOMATION OF BUSINESS PROCESSES IN RECORDING STUDIOS: CHATBOT<br>IMPLEMENTATION AND INFORMATION SECURITY ISSUES<br>Mukhin Maxim, Titova Rosalia .....                                                      | 408        |

|                                                                                                                                                                                                           |            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| ARTIFICIAL INTELLIGENCE IN EDUCATION: TRAINING FOR THE DIGITAL ECONOMY<br>Rakovsky Oleg, Anshakov Artem .....                                                                                             | 410        |
| TRAINING AND PROFESSIONAL DEVELOPMENT INFORMATION SECURITY SPECIALISTS<br>IN THE REGIONS OF RUSSIA<br>Renskov Dmitry .....                                                                                | 412        |
| GAMIFICATION OF THE EDUCATIONAL PROCESS IN IT UNIVERSITIES:<br>APPLICATION RISKS<br>Smorodin Gennadii, Faizullin Radmir .....                                                                             | 414        |
| <b>YOUTH SCIENTIFIC SCHOOL "ECOSYSTEM OF SAFE URBAN DIGITAL SERVICES" .....</b>                                                                                                                           | <b>415</b> |
| DIGITAL INCLUSION AND CYNERSECURITY FOR PEOPLE WITH HEALTH CONDITIONS<br>AND SOCIOCULTURAL ENVIRONMENT IN RUSSIA<br>Barandova Tatiana .....                                                               | 415        |
| DIGITAL TRUST: FACTORS OF SUSTAINABILITY OF INTERACTION BETWEEN<br>CITIZENS AND AUTHORITIES THROUGH DIGITAL PLATFORMS<br>Kutepova Daria .....                                                             | 417        |
| SOCIAL WELL-BEING ANALYSIS: HOW THE REGIONAL MANAGEMENT CENTER<br>BECOMS A «SIGNAL SYSTEM» OF PUBLIC OPINION<br>Negulyaev Stanislav .....                                                                 | 418        |
| THE PERCEPTION OF THE SECURITY OF MOBILE APPLICATIONS<br>WITH AI IN USER COMMENTS<br>Nizomutdinov Boris .....                                                                                             | 420        |
| A COMPARATIVE ANALYSIS OF RUSSIAN RESIDENTS' ID CARDS<br>IN THE CONTEXT OF PROVIDING SOCIAL SUPPORT<br>Raits Valeriy .....                                                                                | 424        |
| <b>YOUTH SCIENTIFIC SCHOOL "SAFE INTELLIGENT INFORMATION SYSTEMS AND<br/>TECHNOLOGIES" .....</b>                                                                                                          | <b>426</b> |
| MEDICAL INTELLIGENT SYSTEM FOR PERSONALIZED REHABILITATION<br>OF FACIAL MUSCULATURE AFTER STROKE<br>Avdeeva Taisiya, Zharanova Anastasia, Litvinov Vladislav .....                                        | 426        |
| INTELLIGENT SYSTEM FOR PREVENTING FRAUDULENT TRANSACTIONS<br>Asadullaev Vladislav, Filippov Felix .....                                                                                                   | 428        |
| COUNTERING HULK-TYPE ATTACKS IN INFORMATION AND COMPUTING NETWORKS<br>Babanov Zach, Maksimenko Sergey, Shevchenko Aleksandr .....                                                                         | 429        |
| ADAPTIVE DECENTRALIZED DATA TRANSMISSION WITH FRAGMENTED ENDCRYPTION,<br>MULTI-ROUTING AND SECTOR ADDRESSING<br>Harokhau Dzmitry, Labkovskaya Rimma .....                                                 | 430        |
| ASSESSMENT OF THE EFFECTIVENESS OF INFORMATION NETWORK MONITORING<br>AND MANAGEMENT SYSTEMS IN THE CONTEXT OF DYNAMICALLY<br>CHANGING USER LOADS AND REQUIREMENTS<br>Gubin Alexander, Klimova Julia ..... | 432        |
| INFORMATION EFFICIENCY OF IT-PROJECT SUPPORT SYSTEMS<br>Litvinov Vladislav, Orlova Valery .....                                                                                                           | 433        |
| ARTIFICIAL INTELLIGENCE IN EDUCATION: ETHICAL ISSUES<br>AND INFORMATION SECURITY<br>Litvinov Vladislav, Samburova Varvara .....                                                                           | 434        |
| APPLICATION OF DISTANCE LEARNING TECHNOLOGIES IN GRANT WRITING TRAINING<br>Litvinov Vladislav, Litvinova Ekaterina .....                                                                                  | 435        |

|                                                                                                                                                                                                                 |            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| INFORMATION SECURITY OF CYBER-PHYSICAL SYSTEMS IN THE «SMART CITY»<br>ERA: CURRENT REGULATORY CHALLENGES<br>Rakovskiy Oleg, Golaktionov Dmitry .....                                                            | 437        |
| RSSI-BASED LOCALIZATION ACCURACY FOR WIRELESS DEVICES<br>Sinitsyna Olga, Kovzur Maxim, Drepa Vladislav .....                                                                                                    | 438        |
| ANALYSIS OF THE APPLICABILITY OF BYTECODE MODIFICATION METHODS<br>FOR EMBEDDING A DIGITAL WATERMARK IN SCALA PROGRAMS<br>Sokolov Igor .....                                                                     | 439        |
| <b>YOUTH SCIENTIFIC SCHOOL "SAFE COMMUNICATION SYSTEMS" .....</b>                                                                                                                                               | <b>441</b> |
| DIFFICULTIES OF TRANSITION TO NEW GENERATION COMMUNICATION NETWORKS<br>Avetikov Artem, Zadboev Vadim, Timofeev Artyom.....                                                                                      | 441        |
| EVALUATION OF THE EFFECTIVENESS OF AN AUTOMATED OCT IMAGE ANALYSIS SYSTEM<br>Aksenova Lyubov .....                                                                                                              | 443        |
| FRAGMENTATION OF VULNERABILITY DATA AS A CHALLENGE TO INFORMATION<br>SECURITY AND WAYS TO OVERCOME IT<br>Antipina Sofya, Pestov Igor.....                                                                       | 444        |
| PREVENTING EXTERNAL LEAKAGES OF PERSONAL DATA<br>FROM HEALTH MONITORING DEVICES<br>Antropova Lidiya, Zadboev Vadim, Sannikova Polina .....                                                                      | 446        |
| EXPERIMENTAL EVALUATION OF THE PROTECTION LEVEL<br>OF KOTLIN APPLICATIONS AFTER OBFUSCATION<br>Asakov Maksim.....                                                                                               | 448        |
| ANALYSIS OF DIGITAL WATEMARK RESILIENCE IN BYTECODE<br>OF KOTLIN LAMBDA OBJECTS GENERATION TYPE<br>Asakov Maksim, Rubleva Ekaterina.....                                                                        | 449        |
| EVALUATION OF THE EFFECTIVENESS OF ANKEY SIEM NG IN DETECTING DDOS<br>THREATS: POTENTIAL AND DISADVANTAGES<br>Akhrameeva Ksenia, Zhivodovsky Ivan, Zhuravleva Anastasia, Spitsyn Mikhail.....                   | 450        |
| SELECTING A VIRTUALIZATION PLATFORM IN THE CONTEXT OF TECHNOLOGICAL<br>POLARIZATION: A COMPARISON OF GENERAL-PURPOSE<br>AND SPECIALIZED APPROACHES<br>Biryuchevskiy Nikita, Pestov Igor, Mamchenko Kseniia..... | 452        |
| GRAPH MODELING OF THREAT CONNECTION FOR PROACTIVE CYBER RISK FORECASTING<br>Bogdanov Alexey .....                                                                                                               | 453        |
| AUTOMATED VULNERABILITY DETECTION SYSTEM FOR INDUSTRIAL IOT DEVICES<br>Borisenko Ivan, Zhivodovsky Ivan, Markov Alexander.....                                                                                  | 454        |
| PROSPECTS FOR THE APPLICATION OF POST-QUANTUM CRYPTOGRAPHY IN IMT-2030<br>Bryushinin Alexander, Vtorov Oleg, Shevchenko Aleksandr .....                                                                         | 455        |
| SIGNAL MONITORING OF COMMUNICATION LINES TO IDENTIFY CONNECTIONS<br>Vasichkin Sergey .....                                                                                                                      | 457        |
| SPECIALIZED HARDWARE AS TOOLS FOR ENSURING INFORMATION SECURITY<br>IN BIOMETRIC SYSTEMS<br>Veselova Anastasia .....                                                                                             | 459        |
| DIGITAL RESILIENCE OF THE STATE THROUGH PROPRIETARY<br>SECURITY MONITORING PLATFORMS<br>Volostnyh Viktor, Zadboev Vadim, Lipatnikov Valeriy .....                                                               | 460        |

|                                                                                                                                                                                                                      |     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| FEATURES OF MANDATORY INTEGRITY CONTROL IN THE ASTRA LINUX<br>SPECIAL EDITION SPECIAL-PURPOSE OPERATING SYSTEM<br>Grebennikov Timofey.....                                                                           | 461 |
| THREATS AND METHODS OF PROTECTION AGAINST DATA POISONING ATTACKS<br>IN ARTIFICIAL INTELLIGENCE SYSTEMS<br>Gugunishvili Lali, Zhivodovsky Ivan, Shulyndina Maria .....                                                | 463 |
| NRD-LISTS AS A COMPONENT OF INFORMATION SECURITY SOLUTIONS<br>Gudakov Anton, Minyaev Andrey, Skorykh Mark.....                                                                                                       | 465 |
| PROTECTION OF INFORMATION SYSTEMS FROM NETWORK INTELLIGENCE<br>BY TRAFFIC ANALYSIS METHODS<br>Dzegovskii Vladislav, Zhivodovsky Ivan, Shadrin Ilya .....                                                             | 466 |
| ZVIRT AS A SECURE VIRTUALIZATION PLATFORM<br>Dyusmetova Azaliya, Pestov Igor, Alekseeva Kseniya .....                                                                                                                | 467 |
| ADAPTATION OF SECURE MOBILE APPLICATION DEVELOPMENT METHODOLOGY<br>FOR TEAMS OF DIFFERENT SCALES<br>Emelyanov Nikolai, Kovtsur Maxim .....                                                                           | 468 |
| ENSURING INFORMATION SECURITY BASED ON FOG COMPUTING<br>Zozulya Gleb, Shevchenko Aleksandr .....                                                                                                                     | 470 |
| IMPACT OF EXTERNAL THREATS ON PERSONAL DATA<br>Zadboev Vadim, Kot Irina, Saitov Nikita .....                                                                                                                         | 471 |
| MALWARE ATTACK PREDICTION TOOL<br>Zadboev Vadim, Lipatnikov Valeriy, Sadovnikov Vladimir .....                                                                                                                       | 472 |
| MQTT VULNERABILITY ANALYSIS IN IOT<br>Zadboev Vadim, Shashin Mikhail, Jakobson Dmitriy .....                                                                                                                         | 474 |
| VIRTUALIZATION OF FIREWALLS AS A TOOL FOR INCREASING FAULT TOLERANCE<br>AND SECURITY OF CORPORATE NETWORKS<br>Zuev Dmitry .....                                                                                      | 475 |
| ENSURING INFORMATION SECURITY OF SMART PARKING SYSTEMS<br>Kirkum Gleb, Sirgazinov Timur, Shevchenko Aleksandr .....                                                                                                  | 477 |
| DECOMPOSITION OF SECURITY ASSESSMENT REQUIREMENTS<br>FOR CII FACILITIES BY FUNCTIONAL PURPOSE<br>Kiselev Nikolay .....                                                                                               | 479 |
| PRACTICE OF BUILDING ATTACK-RESISTANT INFRASTRUCTURE BASED<br>ON THE LORAWAN PROTOCOL<br>Krasnikov Daniil, Kovzur Maxim, Nikiforov Alexander .....                                                                   | 481 |
| HOMOMORPHOUS ENCRYPTION AS A DATA PRIVACY PROTECTION<br>Kuklina Margarita, Romanova Alexandra, Shevchenko Aleksandr .....                                                                                            | 482 |
| INFORMATION CRITICAL ASSESSMENT SUPPORT SYSTEMS AS AN ANTI-PHISHING METHOD<br>Lagutina Svetlana, Vitkova Lidia .....                                                                                                 | 483 |
| METHODOLOGY FOR ROBUSTNESS ASSESSMENT OF THE RAW KEY GENERATION METHOD<br>IN A KEY DISTRIBUTION PROTOCOL BASED ON THE DIFFERENCE OF TRANSMITTED<br>SAMPLES USING A LOOKUP TABLE-BASED ATTACK<br>Lapshin Alexey ..... | 485 |
| MODELING CLIENT OS NETWORK BEHAVIOR TO IMPROVE IDS EFFICIENCY<br>Legkodymov Daniil, Staroverov Andrey, Shevchenko Alexander, Shchogolev Yefim .....                                                                  | 486 |

|                                                                                                                                                                                                                                    |            |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| SECURITY ASSESSMENT OF THE ACCESS RESTRICTION MODEL IN KUBERNETES:<br>FROM CONFIGURATION AUDIT TO ATTACK VECTOR SEARCH<br>Mastenitsa Evgeniy .....                                                                                 | 488        |
| STATIC ANALYSIS METHODS FOR IDENTIFYING DEFECTS AND IMPROVING CODE CLEANLINESS<br>Orlova Daria .....                                                                                                                               | 489        |
| IOT INFORMATION SECURITY IN 6G NETWORKS<br>Pivovarov Daniil, Timofeev Lavr, Shevchenko Aleksandr .....                                                                                                                             | 490        |
| RESEARCH OF NEURAL NETWORK TECHNOLOGIES AS A TECHNOLOGY<br>FOR AUTOMATED INCIDENT RESPONSE<br>Platonov Aleksei, Kovzur Maxim, Minyaev Andrei .....                                                                                 | 491        |
| INTEGRATION OF SMART MANUFACTURING AND CYBERSECURITY CONCEPTS<br>INTO AUTOMATED PROCESS CONTROL SYSTEMS<br>Pozishev Sergey, Shterenberg Stanislav .....                                                                            | 492        |
| BEHAVIORAL MODELING WITH FINITE AUTOMATA IN INTRUSION DETECTION SYSTEMS: SEMANTIC<br>ANALYSIS OF SYSTEM EVENTS IN LINUX ENVIRONMENTS<br>Potemkina Yuliya .....                                                                     | 494        |
| MODERN DEVELOPMENT VECTORS OF ACCESS CONTROL SYSTEMS IN WEB APPLICATIONS<br>Rogatykh Ksenia .....                                                                                                                                  | 495        |
| A METHOD FOR COMPREHENSIVE ASSESSMENT OF THE LEVEL OF MATURITY<br>OF AN ORGANIZATION'S INFORMATION SECURITY SYSTEM<br>Sakharov Dmitry, Birikh Ernest, Gavrilov Pavel .....                                                         | 497        |
| COMPARATIVE STUDY OF DIGITAL WATERMARK PERSISTENCE IN BYTECODE<br>OF PROGRAMMING LANGUAGES COMPILED FOR JAVA VIRTUAL MACHINE<br>Sokolov Igor .....                                                                                 | 498        |
| TRADE-OFFS AND RISKS WHEN IMPLEMENTING DISTRIBUTED STORAGE IN SECURE<br>VIRTUALIZED ENVIRONMENTS: THE EXPERIENCE OF USING CEPH<br>IN THE SOFTWARE COMPLEX OF VIRTUALIZATION TOOLS «BREST»<br>Stroilo Anna, Tsvetkov Alexandr ..... | 500        |
| SECURITY THREATS IN ADAPTIVE ARTIFICIAL INTELLIGENCE AGENTS<br>Trofimov Evgeniy, Vitkova Lidiya .....                                                                                                                              | 501        |
| NEW WAYS TO PROTECT INFORMATION AND DATA IN THE FIELD<br>OF TELEPRESENCE SERVICES<br>Ushakov Igor, Shterenberg Stanislav, Pankov Arseniy .....                                                                                     | 503        |
| INFLUENCE OF ARTIFICIAL NEURAL NETWORK ARCHITECTURE<br>ON NETWORK ATTACKS DETECTION<br>Filonov Artyom, Katasonov Aleksandr .....                                                                                                   | 504        |
| USING THE EOF METHOD TO HIDE DATA IN IMAGES: POSSIBILITIES AND LIMITATIONS<br>Khimich David .....                                                                                                                                  | 505        |
| DETECTION OF NETWORK TRAFFIC ANOMALIES DURING PACKET DATA<br>TRANSMISSION IN PRE-5G MOBILE NETWORKS<br>Cherkashin Artem .....                                                                                                      | 507        |
| EFFECTIVENESS OF WAZUH FOR LAN ATTACK DETECTION<br>Sharifov Roman .....                                                                                                                                                            | 508        |
| RESEARCH ON BUILT-IN INFORMATION SECURITY MECHANISMS<br>IN BETAFLIGHT SOFTWARE<br>Yanis Nikolay, Rumyantsev Alexander .....                                                                                                        | 509        |
| <b>CONTENTS .....</b>                                                                                                                                                                                                              | <b>533</b> |